数据库安全漏洞浅析

数据库漏洞的种类繁多和危害性严重是数据库系统受到攻击的主要原因，通过研究数据库漏洞分类，有助于人们对漏洞的深入理解并加以预防和避免。

美国 Verizon 就“核心数据是如何丢失的”做过一次全面的市场调查，结果发现，75%的数据丢失情况是由于数据库漏洞造成的，这说明数据库的安全非常重要。

据 CVE 的数据安全漏洞统计， Oracle 、 SQL Server、 MySQL 等主流数据库的漏洞逐年上升，以 Oracle 为例，当前漏洞总数已经超过了 1200 多个。

数据库安全漏洞从来源上，大致可以分为四类：缺省安装漏洞、人为使用上的漏洞、数据库设计缺陷、数据库产品的 bug。

1、缺省安装漏洞

- 数据库安装后的缺省用户名和密码

在主流数据库中往往存在若干缺省数据库用户，并且缺省密码都是公开的，攻击者完全可以利用这些缺省用户登录数据库。例如，Oracle 中有 sys、system、sysman、scott 等 700 多个缺省用户；MySQL 本机的 root 用户可以没有口令；网络上主机名为 build 的 root 和用户可以没有口令。

- 数据库安装后的缺省端口号

在主流数据库中缺省端口号是固定的，如 Oracle 是 1521、SQL Server 是 1433、MySQL 是 3306 等。

- 数据库安装后低安全级别设置

数据库安装后的缺省设置，安全级别一般都较低。

如 MySQL 中本地用户登录和远程 build 主机登录不校验用户名密码。

如 Oracle 中不强制修改密码、密码的复杂度设置较低、不限定远程链接范围、通讯为明文等。

● 启用不必要的数据库功能

在数据库的缺省安装中为了便于使用和学习，提供了过量的功能和配置。如 Oracle 安装后无用的示例库、有威胁的存储过程； MySQL 的自定义函数功能。

典型数据库泄密案例：Korea 会展中心数据库被入侵

2011 年 5 月，黑客入侵 Korea 会展中心数据库，在网上爆出其中大量的客户资料数据，并展示数据库操操作过程。

黑客首先通过端口扫描技术，检测出该服务器上开放着 1521 端口（Oracle 数据库的缺省端口），首先探明该主机便是数据库服务器。接着利用扫描程序，检测到缺省系统用户 dbsnmp 并未被锁定，且保留着数据库安装时的缺省密码。

之后黑客利用权限提升的漏洞，将 dbsnmp 用户的权限提升至 DBA，开始了数据库访问之旅。

2、人为使用漏洞

● 过于宽泛的权限授予

在很多系统维护中，数据库管理员并未细致地按照最小授权原则给予数据库用户授权，而是根据最为方便的原则给予了较为宽泛的授权。

例如，一个普通的数据库维护人员被授予了任意表的创建和删除、访问权限，甚至是给予 DBA 角色；

例如，一个大学管理员在工作中只需要能够更改学生的联系信息，不过他可能会利用过高的数据库更新权限来更改分数。

- 口令复杂度不高

弱口令：非默认的数据库口令也是不安全的，通过暴力破解，攻击者不断地输入用户名和密码组合，直到找到可以登录的一组。暴力过程可能是靠猜想，也可 能是系统地枚举可能的用户名/密码组合。通常，攻击者会使用自动化程序来加快暴力过程的速度。口令破解的工具有很多，并且通过 Google 搜索或 sectools.org 等站点就可以轻易地获得，这样就会连接到 Cain、Abel 或 John the Ripper 等流行的工具。

密码曝光：一些公众权限的存储过程、表的调用会导致密码曝光。例如，通过执行公众权限的存储过程 msdb.dbo.sp_get_sqlagent_properties 可以获得 SQL Agent 密码；通过查询公众权限的表 RTblDBMProps 可查看 DTS 密码；Microsoft SQL Server 允许本地用户通过数据转换服务（DTS）包属性对话框获得数据库密码。

例如，Oracle 10.1 及早期版本，sysman 用户的密码明文存储在 emoms.properties 中，10.2 后，虽加密存储，但密钥也存在该文件中，且用 DES 算法，很容易解密。

因此建议管理员细致地按照最小授权原则给予数据库用户授权；数据库用户口令长度应大于等于 10，并且应该包括字母和数字，应该通过一个口令检验函数来实施这一点。

3、数据库设计缺陷

- 明文存储引起的数据泄密

在当前的主流数据库中，数据以明文形式放置在存储设备中，存储设备的丢失将引起数据泄密风险。

数据库数据文件在操作系统中以明文形式存在，非法使用者可以通过网络、操作系统接触到这些文件，从而导致数据泄密风险。

通过 UE 这样的文本工具即可得到部分明文的信息，通过 DUL/MyDUL 这样的工具能够完全实现将数据文件格式化导出。

典型数据库泄密案例：7 天酒店数据库被盗

会员人数超过 1650 万，酒店总数逼近 600 家，在美国纽约证券交易所上市的 7 天连锁酒店集团无疑是国内经济型连锁酒店集团的龙头企业之一，但更多人所不知道的是，从去年开始，7 天酒店在国内黑客圈中成了“明星”。

黑客通过“刷库”直接盗走整个数据库数据。即黑客利用企业网站存在的漏洞入侵数据库服务器，直接将整个数据库文件拷贝，通过 DUL/MyDUL 这种类似的工具将所有二进制方式存储的数据还原成清晰地格式化数据。

- SYSDBA、DBA 等超级用户的存在

在数据库中，以 sys 和 sa 为代表的系统管理员，可以访问到任何数据；除了系统管理员，以用户数据分析人员、程序员、开发方维护人员为代表的特权用户，在特殊的时候，也需要访问到敏感数据，从而获得了权限。这些都为数据的泄密留下了极大的隐患。

例如，掌握特权用户口令的维护人员，进入了 CRM 系统，只需具有对数据库的只读性访问权限，这样，这个用户就可以访问读取数据库内的任何表，包括信用卡信息、个人信息。

- 无法鉴别应用程序的访问是否合法

对于合法的数据库用户，通过合法的业务系统访问数据是正常的行为，但是数据库的一个缺陷在于，无法鉴别应用程序的合法性。

在现实系统维护或开发过程中，应用系统后台使用的合法数据库用户，常由于人为因素或管理不善，用户名及口令很容易泄露给第三方，第三方则可以通过命令行或管理工具直接访问密文数据，批量窃取数据。

典型数据库泄密案例：陕西移动 1400 万手机用户个人信息泄漏

今年 3 月以来，周双成利用职务之便，多次侵入陕西移动用户数据库，盗取手机用户个人信息，贩卖给侦探公司。

周双成利用工作之便，能在研发和维护系统过程中获知数据库口令，数据库口令泄漏后，完全可以绕开合法的业务系统，直接使用该用户通过其他程序（自己编写的木马程序）定期访问数据库，进而窃取数据库中的客户隐私信息。

4、数据库产品 bug

- 缓冲区溢出

这类漏洞是由于不严谨的编码，使数据库内核中存在对于过长的连接串、函数参数、SQL 语句、返回数据不能严谨的处理，造成代码段被覆盖。

通过覆盖的代码段，黑客可以对数据库服务器进行各种操作，最常见的是使数据库崩溃，引起拒绝服务。

例如，SQL Server 中利用缓冲区溢出，攻击者可以通过以下函数或存储过程执行任意代码：RAISERROR、FORMATMESSAGE、 xp_sprintf、sp_Mscopyscriptfile、xp_sqlinventory、xp_sqlagent_monitor、sp_OACreate、sp_OAMethod、sp_OAGetProperty、sp_OASetProperty、sp_OADestroy；另

外，xp_peekqueue、xp_displayparamstmt、xp___execresultset 等 40 多个函数或扩展存储过程也存在缓冲 区溢出。

● 拒绝服务攻击漏洞

数据库中存在多种漏洞，可以导致服务拒绝访问，如命名管道拒绝服务、拒绝登录、RPC 请求拒绝服务等。

例如 Microsoft SQL 7.0 服务允许一个远程攻击者通过不正确格式的 TDS 数据包引起拒绝服务；本地或远程用户通过向命名管道发送一个长请求引发拒绝服务。

例如 MySQL 中 Data_format()函数在处理用户提交的参数时存在漏洞，畸形的参数数据会导致 MySQL 服务器崩溃。

● 权限提升漏洞

黑客攻击者可以利用数据库平台软件的漏洞将普通用户的权限转换为管理员权限。漏洞可以在存储过程、内置函数、协议实现甚至是 SQL 语句中找到。

例如，Oracle 中一系列系统对象如 PL/SQL 包，缺省赋予了 Public 角色的执行权限，借助这些包执行注入了” grant dba to user”的函数或过程，或直接作为参数执行即可。有 PUBLIC 执行权限的包共计 30 多个，例 如：ctxsys.driload.validate_stmt（ ）将 grant 语句作为参数即可完成权限提升。

例如，在 SQL Server 中，通过 Job 输出文件覆盖，没有权限的用户可以创建 job 并通过 SQL Server 代理的权限提升执行该 job。

例如，一个金融机构的软件开发人员可以利用有漏洞的函数来获得数据库管理权限。使用管理权限，恶意的开发人员可以禁用审计机制、开设伪造的账户以及转账。