数据库安全风险行为

目录

[1. 数据库安全风险行为 2](#_Toc531)

[1.1. Sql注入SQLi）攻击行为 2](#_Toc19705)

[1.2. . 过多的、不适当的和未使用的特权 2](#_Toc13621)

[1.3. 2. 权限滥用（数据库系统管理员和开发人员）行为 2](#_Toc28970)

[1.4. 3.Web 应用程序风险行为 3](#_Toc12545)

[1.5. 4. 审计线索不足行为 3](#_Toc24907)

[1.6. 5. 不安全的存储介质 3](#_Toc24626)

[1.7. 侵犯隐私行为 3](#_Toc22170)

[1）身份认证安全问题 3](#_Toc29367)

[· 无密码的身份认证安全问题 3](#_Toc22098)

[· 有密码的身份认证安全问题 3](#_Toc8667)

[2）权限控制 3](#_Toc16801)

[3）通讯加密 4](#_Toc27360)

[4）审计 4](#_Toc26212)

[5）数据加密 4](#_Toc6977)

[6）NoSQL注入 4](#_Toc7896)

[7）自身安全漏洞 4](#_Toc9274)

[1.8. 糟糕的加密与数据泄露密不可分 2 5](#_Toc16275)

[1.9. 数据库被盗 2 5](#_Toc5951)

[1.10. 功能中的缺陷成为了数据库安全问题 2 5](#_Toc20099)

[1.11. 弱而复杂的数据库基础架构 2 5](#_Toc31631)

[1.12. 无限的管理访问 = 糟糕的数据保护 3 5](#_Toc4818)

[1.13. 密钥管理不足 3 5](#_Toc27914)

[1.14. 数据库中的不规范 3 4 5](#_Toc19663)

[1.15. 按照发生的可能性排序 1. 人为误操作，删除数据，更改数据 ==>可通过定期备份解决 5](#_Toc14055)

[1.16. 2. 数据库本身故障。 数据库当机。===> 可通过高可用性解决，RAC, HA, Dataguard。 5](#_Toc7769)

[1.17. 3. 服务器硬件故障 ==> 同上 5](#_Toc28936)

[1.18. 4 . 黑客攻击 ==> 可通过定期安装安全补丁，使用符合安全策略的密码等手段解决 5](#_Toc12120)

[1.19. 5. 灾难: 火山，地震，海啸。机房起火。失窃。 ===》 可以通过异地备份，或者祈祷来解 5](#_Toc7420)

[2. Ref 6](#_Toc14154)

# 数据库安全风险行为

## Sql注入SQLi）攻击行为

## . 过多的、不适当的和未使用的特权

当您授予某人超出其工作职能的数据库特权时，这些特权可能会被滥用。例如，其工作能力是需要更新员工休假信息的 HR，可能会利用过多的数据库特权，对同事或高管的薪资数据进行未经授权的查询。

## 2. 权限滥用（数据库系统管理员和开发人员）行为

在每个企业中人们都使用数据库服务帐户来访问数据库，并且这些用户滥用这些特权服务帐户来直接访问敏感数据，从而绕过了应用程序界面。

此外，某些“特权用户”可能会出于未经授权的目的滥用合法的数据库特权。组织中的某些用户组由于其职业和活动而有权访问整个数据库。特权用户的两个主要类别是数据库系统管理员和开发人员

当 DBA 直接通过数据库而不是应用程序界面访问应用程序数据时，他绕过了应用程序日志记录和检索限制，并避免了应用程序权限和安全性机制。

当某个使用防泄露方案的客户端收到以下警告：受信任的 DBA 已直接通过数据库而不是通过某应用程序入口访问了此应用程序表中的敏感数据，这些表包含 DBA 不应访问的财务信息。这一发现清楚地说明了内部威胁的风险。开发人员通常可以完全访问生产数据库，质量团队可以快照数据库以进行测试，而工程师可以调试实时生产系统。在这些情况下，敏感数据都容易受到特权滥用的影响。

## 3.Web 应用程序风险行为

## 4. 审计线索不足行为

## 5. 不安全的存储介质

## ****侵犯隐私行为****

尽管我们专注于安全性，但是隐私问题也不容忽视。以医疗大数据平台为例，提供商可以共享患者数据。患者可以访问系统获取遗传信息，然后再访问有关药物信息的系统。

分析此数据的应用程序可以将信息关联起来，以找到与遗传和健康有关的购买趋势。问题在于，最初插入数据时未考虑这种类型的相关性。

因此，数据未被匿名化脱敏，从而可以从更大的趋势图中查明特定的个人。这将违反包括 HIPAA 和 GDPR 在内的多项法规。

**1）身份认证安全问题**

**·**无密码的身份认证安全问题

由于NoSQL中默认没有用开启户身份认证机制，所以任何用户都可以伪装成合法用户来访问数据库，并对数据库中的数据进行各种操作。如2016年底至2017年初兴起的一股针对NoSQL数据库的勒索行动，就是利用无身份认证登陆上NoSQL数据库实施敲诈勒索，这只是此安全隐患最简单的利用方式。很多时候黑客会以NoSQL数据库为跳板入侵NoSQL数据库所在的服务器，甚至整个网络环境。目前，最直接的解决方法就是给NoSQL加用户名和密码。

**·**有密码的身份认证安全问题

NoSQL出于性能考量，默认不设置用户名和密码。要解决身份认证安全问题，一般采取两种方法。一种是使用NoSQL数据库自身支持的简单身份验证。通过客户端获取用户名和密码，然后和数据库中对应的记录进行比对，吻合则批准登录。该方法在抗暴力破解和网络窃取上非常差，一旦用户数量过多会引起性能的严重下降，所以部分NoSQL数据库不支持多用户登录。

另一种解决方案是以Hbase为代表，引入成熟的身份认证机制Kerberos来完成身份认证工作。该方式较适合以计算为主业的NoSQL数据库，对于要求执行效率和以大量查询为主要的业务并不适合。随着用户数量增长，并发量不断提高，KCD（密钥奋发中心）很快会成为整个业务流程的瓶颈。

**2）权限控制**

NoSQL数据库不仅缺乏身份验证，更缺乏对每个数据库用户的权限控制。很多NoSQL数据库，把自己当作“应用数据库”去设计，完全不关心数据库用户之间的权限区别，导致任意用户都相当于ORACLE数据库的sys用户。这种权限的混乱可能导致应用侧、运维侧两个层面的三种安全风险：1、缺乏命令权限控制；2、缺乏集合访问权限控制；3、缺乏集合内部数据访问控制。

NoSQL中有两类权限，一类是调用脚本的权限；另一类是对数据库系统的权限。Redis在这部分做得较差，任意用户都可以调用这两类权限，导致数据库面临安全威胁。一些重视安全的NoSQL数据库具备一定的访问控制能力，但仍缺乏细粒度的访问控制能力。

**3）通讯加密**

NoSQL数据库不仅身份验证是明文传输，后面的请求和结果集同样也是明文传输。这会导致户隐私数据、系统敏感信息在传输过程被窃取。解决通讯加密一般会提供一个附加的SSL安全层，但ssl安全层会拖慢整个业务的执行速度。后文会给出相应解决方案。

**4）审计**

NoSQL数据库缺乏审计能力，部分NoSQL数据库可以通过配置添加日志监控来完成一部分审计功能。通过日志的记录来判断整个流程中是否存在问题。这种日志的记录缺乏特征的判断和自动提示的功能。后面我们会用NoSQL审计产品完善审计功能的缺失。

**5）数据加密**

NoSQL数据库缺乏对数据的存储保护，所有数据均是明文形式存储，超管可以不经过用户允许直接查看、修改用户在云端保存的文件，很容易造成数据泄露。因此，需要常态保持加密，只允许具有固定身份的用户拿到明文，这样既保护了数据安全又强化了数据库权限控制。

**6）NoSQL注入**

虽然NoSQL数据库不再支持sql语句，也就没有了sql注入的威胁，但存在另外一种威胁——NoSQL注入威胁。NoSQL注入和其他注入类攻击类似，能获得数据库中整个集合（表）的信息，甚至通过改变语义，获得其他集合（表）中的敏感信息。目前已发现的SQL注入有重言式、联合查询、JavaScript注入、背负式查询四种。

**7）自身安全漏洞**

除了上述由于设计理念和web导致的安全风险外，NoSQL数据库本身也存在一些安全漏洞。主要集中在三方面：1、泄露敏感数据；2、越权操作；3、录调用的函数存在缓冲区溢出漏洞，会导致服务宕机。解决方法有二：1、及时打补丁；通过漏洞防护技术进行防护。

数据库安全问题？这里有10个最常见的 1

## 糟糕的加密与数据泄露密不可分 2

## 数据库被盗 2

## 功能中的缺陷成为了数据库安全问题 2

## 弱而复杂的数据库基础架构 2

## 无限的管理访问 = 糟糕的数据保护 3

## 密钥管理不足 3

## 数据库中的不规范 3 4

## 按照发生的可能性排序 1. 人为误操作，删除数据，更改数据 ==>可通过定期备份解决

## 2. 数据库本身故障。 数据库当机。===> 可通过高可用性解决，RAC, HA, Dataguard。

## 3. 服务器硬件故障 ==> 同上

## 4 . 黑客攻击 ==> 可通过定期安装安全补丁，使用符合安全策略的密码等手段解决

## 5. 灾难: 火山，地震，海啸。机房起火。失窃。 ===》 可以通过异地备份，或者祈祷来解

# Ref

七大维度谈NoSQL数据库安全风险 - 嘶吼 RoarTalk – 回归最本质的信息安全,互联网安全新媒体,4hou.com.html

数据库安全问题？这里有10个最常见的 - 掘金.html