数据库系统安全

数据库安全概况
数据库安全机制与实现技术
Oracle数据库安全分析与防护
MS SQL数据库安全分析与防护
MySQL数据库安全分析与防护
国产数据库安全分析与防护

文老师软考教育

数据库安全概况

文老师软考教育

◆数据库安全概念：数据库是网络信息系统的基础性软件，承载着各种各样的数据，成为应用系统的支撑平台。数据库安全是指数据库的机密性、完整性、可用性能够得到保障，其主要涉及数据库管理安全、数据安全、数据库应用安全以及数据库运行安全。

◆数据库安全威胁：数据库所处的环境日益开放，所面临的数据库安全威胁日益增多，包括：
(1)授权的误用(Misuses of Authority)。合法用户越权获得他们不应该获得的资源，窃取程序或存储介质，修改或破坏数据。授权用户将自身的访问特权不适当地授予其他用户，导致系统安全策略受到威胁，使用户数据泄露。

(2)逻辑推断和汇聚(Logical Inference and Aggregation)。利用逻辑推理，把不太敏感的数据结合起来可以推断出敏感信息。进行逻辑推断也可能要用到某些数据库系统以外的知识。与逻辑推断紧密相关的是数据汇聚安全问题，即个别的数据项是不敏感的，但是当足够多的个别数据值收集在一起时，就成为敏感的数据集。

(3)伪装(Masquerade)。攻击者假冒用户身份获取数据库系统的访问权限。

(4)旁路控制(Bypassing Controls)。在数据库设置后门，绕过数据库系统的安全访问控制机制。

数据库安全概况

(5)隐蔽信道(Covert Channels)。通常储存在数据库中的数据经由合法的数据信道被取出。与正常的合法信道相反，隐蔽信道利用非正常的通信途径传输数据以躲避数据库安全机制的控制，如共享内存、临时文件。

(6) SQL注入攻击(SQL Injection)。攻击者利用数据库应用程序的输入未进行安全检查的漏洞，欺骗数据库服务器执行恶意的SQL命令。SQL注入攻击常常导致数据库信息泄露，甚至会造成数据系统的失控。

(7)数据库口令密码破解。利用口令字典或手动猜测数据库用户密码，以达到非授权访问数据库系统的目的。互联网常见的黑客攻击技术手段有“撞库”，其技术原理就是通过收集互联网已泄露的用户+口令密码信息，生成对应的字典表，尝试批量登录其他网站后，得到一系列可以登录的用户。

(8)硬件及介质攻击。对数据库系统相关的设备和存储介质的物理攻击。

数据库安全概况

文老师软考教育

◆数据库安全隐患：

1. 数据库用户账号和密码隐患。虽然多数数据库提供基本安全功能，但是没有机制来限制用户必须选择健壮的密码。多数数据库系统有公开的默认账号和默认密码。

2. 数据库系统扩展存储过程隐患。多数数据库系统提供了“扩展存储过程”的服务以满足数据库管理，但是这也成为数据库系统的后门。

3. 数据库系统软件和应用程序漏洞。

4. 数据库系统权限分配隐患。

5. 数据库系统用户安全意识薄弱。

6. 网络通信内容是明文传递。利用数据库和应用程序之间网络通信内容未经加密的漏洞，网络窃听者窃取诸如应用程序特定数据或数据库登录凭据等敏感数据。

7. 数据库系统安全机制不健全。导致安全策略无法实施。

数据库安全概况

◆数据库安全需求：数据库系统的安全目标是保护数据库系统的安全运行及数据资源的安全性。包括：

1．数据库标识与鉴别。用于数据库用户身份识别和认证。

2．数据库访问控制。对数据资源及系统操作进行访问授权及违规控制。数据库系统一般提供自主访问控制、强制访问控制、角色访问控制等多种访问控制模式。

3．数据库安全审计。按照审计安全策略，对相关的数据库操作进行记录，形成数据库审计文件。审计记录的主要信息包括审计的操作类型、执行操作的用户标识、操作的时间、客体对象等用户行为相关信息。

4．数据库备份与恢复。当数据库系统出现故障时，可以实现对备份数据的还原以及利用数据库日志进行数据库恢复重建。

5．数据库加密。对数据库中的敏感数据进行加密处理，并提供密钥管理服务。

6．资源限制。防止授权用户无限制地使用数据库服务器处理器(CPU)、共享缓存、数据库存储介质等数据库服务器资源，限制每个授权用户／授权管理员的并行会话数等功能。

7．数据库安全加固。对数据库系统进行安全漏洞检查和修补，防止安全漏洞引入数据库系统。

8．数据库安全管理。数据库系统提供安全集中管理机制，实现数据库的安全策略集中配置和管理。

文老师软考教育

数据库安全机制与实现技术

◆数据库安全机制：各安全机制的功能如表所示。

安全机制名称	安全功能
标识与鉴别	用户属性定义、用户，主体绑定、鉴别失败处理、秘密的验证、鉴别的时机、多重鉴别机制设置等
访问控制	会话建立控制、系统权限设置、数据资源访问权限设置
安全审计	审计数据产生、用户身份关联、安全审计查阅、限制审计查阅、可选审计查阅、选择审计事件
备份与恢复	备份和恢复策略设置、备份数据的导入和导出
数据加密	加密算法参数设置、密钥生成和管理、数据库加密和解密操作
资源限制	持久存储空间分配最高配额、临时存储空间分配最高配额、特定事务持续使用时间或未使用时间限制
安全加固	漏洞修补、弱口令限制
安全管理	安全角色配置、安全功能管理

数据库安全机制与实现技术

◆数据库加密：数据库加密方式主要分为两种类型：一是数据库网上传输的数据，通常利用SSL协议来实现；二是数据库存储的数据，通过数据库存储加密来实现。

◆按照加密组件与数据库管理系统的关系，数据库存储加密可以分成两种加密方式：库内加密和库外加密。库内加密是指在DBMS内部实现支持加密的模块。库外加密指在DBMS范围之外，由专门的加密部件完成加密／解密操作。

◆数据库存储加密的常用技术方法有基于文件的数据库加密技术、基于记录的数据库加密技术、基于字段的数据库加密技术。其中，基于文件的数据库加密技术将数据库文件作为整体，对整个数据库文件进行加密，形成密文来保证数据的机密性。基于记录的数据库加密技术将数据库的每一个记录加密成密文并存放于数据库文件中。基于字段的数据库加密技术加密数据库的字段，以不同记录的不同字段为基本加密单元进行加密。

◆数据库防火墙：根据预定义的禁止和许可策略让合法的SQL操作通过，阻断非法违规操作，形成数据库的外围防御圈，实现SQL危险操作的主动预防、实时审计。面对来自外部的入侵行为，数据库防火墙提供SQL注入禁止和数据库虚拟补丁包功能。通过虚拟补丁包，数据库系统不用升级、打补丁，即可完成对主要数据库漏洞的防控。

数据库安全机制与实现技术

文老师软考教育

◆数据库防火墙的安全作用主要如下：

(1)屏蔽直接访问数据库的通道。数据库防火墙部署介于数据库服务器和应用服务器之间，屏蔽直接访问的通道，防止数据库隐通道对数据库的攻击。

(2)增强认证。应用程序对数据库的访问，必须经过数据库防火墙和数据库自身两层身份认证。

(3)攻击检测。可实时检测用户对数据库进行的SQL注入和缓冲区溢出攻击，并报警或者阻止攻击行为，记录攻击操作发生的时间，来源IP、登录数据库的用户名、攻击代码等详细信息。

(4)防止漏洞利用。捕获和阻断数据库漏洞攻击行为，如利用SQL注入特征库可以捕获和阻断数据库SQL注入行为。实现虚拟化补丁，保护有漏洞的数据库系统。

(5)防止内部高危操作。可以限定更新和删除影响行、限定无Where的更新和删除操作、限定drop、truncate等高危操作避免大规模损失。

(6)防止敏感数据泄露。可以限定数据查询和下载数量、限定敏感数据访问的用户、地点和时间。

(7)数据库安全审计。对数据库服务器的访问情况进行独立审计，审计信息可以包括用户名、程序名、IP地址、请求的数据库、连接建立的时间、连接断开的时间、通信量大小、执行结果等信息。

数据库安全机制与实现技术

◆数据库脱敏：是指利用数据脱敏技术将数据库中的数据进行变换处理，在保持数据按需使用目标的同时，又能避免敏感数据外泄。数据脱敏指按照脱敏规则对敏感数据进行的变换，去除标识数据，数据实现匿名化处理，从而实现敏感数据的保护。目前，常见的数据脱敏技术方法有屏蔽、变形、替换、随机、加密，使得敏感数据不泄露给非授权用户或系统。

◆数据库漏洞扫描：模拟黑客使用的漏洞发现技术，对目标数据库的安全性尝试进行安全探测分析，收集数据库漏洞的详细信息，分析数据库系统的不安全配置，检查有弱口令的数据库用户。通过数据库漏洞扫描，跟踪监控数据库安全危险状态变化，建立数据库安全基线，防止数据库安全危险恶化。数据库漏洞扫描的商业产品有NGSSQuirrel for Oracle、xSecure-DBScan等。

◆其中，NGSSQuirrel for Oracle可以检查几千个可能存在的安全威胁、补丁状况、对象和权限信息、登录和密码机制、存储过程以及启动过程。NGSSQuirrel提供强大的密码审计功能，包括字典和暴力破解模式。

Oracle数据库安全分析与防护

◆ Oracle数据库安全分析：Oracle数据库提供如下安全机制：

(1)用户认证。除了Oracle数据库认证外，还集成支持操作系统认证、网络认证、多级认证、SSL认证。Oracle数据库的认证方式采用“用户名+口令”，具有口令加密、账户锁定、口令生命期和过期、口令复杂度验证等安全功能。对于数据库管理员认证，Oracle数据库要求进行特别认证，支持强认证、操作系统认证、口令文件认证。网络认证支持第三方认证、PKI认证、远程认证等。

(2)访问控制。Oracle数据库内部集成网络访问控制和数据对象授权控制。Oracle数据库提供细粒度访问控制，如针对select、insert、update、delete等操作，可以使用不同的策略。

(3)保险库。Oracle数据库建立数据库保险库(DV)机制，用于保护敏感数据，具有防止数据系统未授权变更、多因素可信授权、职责隔离、最小化特权的功能。DV机制通过设置安全域和命令规则对特权进行控制。DV机制的命令控制可阻止未授权命令操作，如drop table、alter system。

(4)安全审计和数据库防火墙。Oracle数据库具有对其内部所有发生的活动进行审计的能力。Oracle数据库可审计的活动有3种类型：登录尝试、数据库活动和对象存取。Oracle数据库防火墙提供了SQL语法分析引擎，检查进入数据库的SQL语句，精确地确定是否允许、记录、警告、替换或阻止SQL。Oracle数据防火墙支持白名单、黑名单和基于例外名单的策略。

(5)高级安全功能。Oracle数据库提供透明数据加密和数据屏蔽机制，以保护数据安全。

Oracle数据库安全分析与防护

◆ Oracle安全最佳实践：

(1)增强Oracle数据库服务器的操作系统安全。最小化系统服务，安装最新补丁，关闭不需要的网络通信端口。

(2)最小化安装Oracle，删除不必要的组件。

(3)安装最新的安全补丁。

(4)删除或修改默认的用户名和密码。

(5)启用认证机制。

(6)设置好的口令密码策略。

(7)设置最小化权限。

(8)限制连接Oracle的IP地址。在打补丁的同时限制连接的IP，避免攻击者的IP访问到数据库。

(9)传输加密。Oracle采用的是TNS协议传输数据，在传输过程中不能保证其中的数据不被窃听乃至修改，因此最好对传输进行加密。例如，采用SSL加密机制。

(10)启用Oracle审计。记录所有的用户失败访问和分析安全事件日志。

(11)定期查看Oracle漏洞发布信息，及时修补漏洞。

(12)实施Oracle灾各计划。监测Oracle的安全运行，定期对数据库数据进行备份。针对Oracle的可能安全事件，制定安全应急预案。

MS SQL数据库安全分析与防护

◆ MS SQL安全分析：安全机制主要包括：

(1)用户身份认证。支持Windows认证和混合认证两种方式。Windows认证是默认认证方式。

(2)访问控制。采用基于角色的访问控制机制。其中，SQL Server的角色分为三种类型，即固定服务器角色、固定数据库角色和应用角色。

(3)数据库加密。SQL保密Server提供Transact-SQL函数、非对称密钥、对称密钥、证书、透明数据加密机制。MS SQL Server 2008提供透明数据库加密服务。透明加密使用不同密钥对不同敏感数据进行加密处理，其中密钥类型有服务主密钥、数据库主密钥、数据库密钥。

(4)备份、恢复机制。支持静态备份和动态备份。有四种备份方案：文件和文件组备份、事务日志备份、完全备份、差异备份。而恢复机制有三种模型：简单恢复、完全恢复和批量日志记录恢复。SQL Server系统可运用Transact-SQL语句或企业管理器实现数据的恢复或备份操作。

(5)安全审计。

MS SQL数据库安全分析与防护

◆ MS SQL Server安全最佳实践：

1．设置好的数据库密码安全策略。

2．加强扩展存储过程管理，删除不必要的存储过程。SQL Server的系统存储过程容易被利用来提升权限或进行破坏。为保护SQL Server的安全，删除不必要的存储过程。

3．网上数据加密传输。SQL Server使用的Tabular Data Stream协议用明文传输数据，容易导致数据库敏感数据网上泄露，建议使用SSL协议。

4．修改数据库默认的TCP/IP端口号。更改SQL Server原默认的1433端口，减少攻击者获取数据库端口信息。

5．对SQL数据库访问的网络连接进行IP限制。通过防火墙或Windows操作系统的安全功能对SQL数据库IP连接进行限制，只保证授权的IP能够访问，降低数据库的网络安全威胁来源。

6．启用SQL Server日志审计，记录所有的用户访问和分析安全事件日志。

7．定期查看MS SQL Server漏洞发布信息，及时修补漏洞。

8．保证MS SQL Server的操作系统安全。

9．MS SQL Server安全检测，制定安全容灾备份计划

MySQL数据库安全分析与防护

◆ MySQL安全分析：MySQL提供的安全机制主要包括如下内容：

◆用户身份认证。MySQL支持用户名／口令认证方式。

◆访问授权。MySQL具有5个授权表：user、db、host、tables_priv和columns_priv。通过授权表，MySQL提供非常灵活的安全机制。MySQL具有grant和revoke命令，可以用来创建和删除用户权限，便于分配用户权限。MySQL管理员可以用grant和revoke来创建用户、授权和撤权、删除用户。

◆安全审计。MySQL内置了审计机制，可以记录MySQL的运行状况。

◆ MySQL安全最佳实践：

1．MySQL安装。建立单独启动的用户和组。安装最新的软件包，选择合适的静态参数编译数据库。

2．建立MySQL Chrooting运行环境。形成“沙箱”保护机制，增强系统抗渗透能力。

3．关闭MySQL的远程连接。关闭MySQL的默认监听端口3306，避免增加MySQL的远程攻击风险。

4. 禁止MySQL导入本地文件。禁止MySQL中用“LOAD DATA LOCAL INFILE”命令。

5．修改MySQL的root用户ID和密码

6. 删除MySQL的默认用户和db。删除MySQL的默认数据库test。除了root用户外，其他的用户都去掉。

7．更改MySQL的root用户名，防止口令暴力破解。

8．建立应用程序独立使用数据库和用户账号。要求这些账号只能访问应用程序用到的数据库。

9．安全监测。安全监控MySQL数据库运行，及时修补MySQL数据库漏洞。

10．安全备份，定期备份MySQL数据库系统及数据。

国产数据库安全分析与防护

◆国产数据库概况：国产数据库是指由国家自主研发力量研制的数据库系统，具有较强的可控性和安全性。围绕数据库安全，我国制定了国家标准《信息安全技术数据库管理系统安全技术要求》（GB/T 20273-2019），该标准规定了数据库管理系统的五个安全等级及其所需要的安全技术要求。

◆国产数据库安全分析：

1．国产数据库安全漏洞。

2．国产数据库依赖第三方系统组件的安全。例如Open SSL协议安全漏洞，对国产数据库网络传输数据有安全影响。

3．国产数据库系统安全配置的安全。对国产数据库系统的安全敏感配置不当，构成系统安全威胁。常见的安全配置不当包括未启用国产数据库安全功能、设置数据库弱口令、开放过多的服务端口、使用非安全远程登录工具等。

4. 国产数据库支持平台的安全。国产数据库受制于操作系统而产生的安全问题。例如，操作系统的安全问题导致数据库文件被窃取或破坏，甚至失去控制。

◆国产数据库安全增强措施：

1．国产数据库安全漏洞挖掘及扫描

2．国产数据库加密

3．国产安全数据库

谢谢！