|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| 数据库系统及安全  实验手册 | | | |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  | **学号：** | |  |
|  |  |  |  |
|  | **姓名：** | |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| **网络空间安全学院**  **2022年秋季** | | | |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

实验四、数据库系统安全实验

1. 实验目的
2. 熟悉与掌握数据库安全的基本概念和技术；
3. 了解数据库安全的身份认证与访问控制机制及其使用方法；
4. 了解数据库管理系统安全加固的基本方法；
5. 掌握数据库备份与恢复的基本方法；
6. 了解SQL注入的基本原理和预防方法。
7. 实验要求
8. 本次实验为个人独立实验，作业模板可基于本实验手册，在实验内容后面直接填写实验报告。
9. 作业提交方式：电子版(rar/zip打包)，文件命名格式：[学号]-[姓名]-实验[序号1位数，1--9].rar/zip；作业文件建议使用word或者pdf格式，不接受拍照图片版本。
10. 作业提交到北航网盘：共享目录“DBMS-2022-作业”上传

https://bhpan.buaa.edu.cn:443/link/53C3AF672185198F3381B8E0F83229DF 密码：z0sD

1. 每一个实验内容，根据要求，进行实际操作，并把具体的步骤记录下来，如给出数据操作等SQL语句，结果截图后附在后面。
2. 实验内容
3. 针对第三次实验课选择的实际应用场景，对应用程序访问数据库的用户设计合理的数据库访问权限，基于“最小权限”的原则，要求如下(基于Oracle)：
   1. 不能具有DBA的权限
   2. 不能创建、修改（表结构）和删除（整张表）任何表
   3. 基于应用系统的数据访问需求设置相应的权限
   4. 给出上述所有授权的sql脚本，并作基本验证（结果截图）
4. 设计一个应用程序访问数据库所使用的用户名和密码（不能直接写在代码里，建议使用配置文件）存储与解析的解决方案，解决明文存储问题，给出详细的方案描述。
5. 针对Oracle数据库，对其进行基本安全加固，要求如下：
   1. 在安装数据库的机器上，要求任何用户登录数据库必须提供密码，不可以dba直接登录数据库(如 sqlplus / as sysdba)；
   2. 限制用户密码的复杂度（包括字母、数字和特殊字符等），设置每隔60天需要重新修改密码，如果用户密码连续输错3次就锁定用户（不能再登录），设置用户登录session空闲超时间隔为10分钟。
   3. 限制应用程序从某些固定的IP地址访问数据库服务器。
6. 对某一使用的数据库（可以是第一次实验的销售数据库，也可以是第三次实验的应用场景数据库），采用当前的用户对数据库逻辑数据备份与恢复，然后再使用与备份数据库不一样的用户名进行数据恢复(使用Oracle IMPDP/EXPDP进行备份与恢复)，给出执行结果与验证截图。（提示：为了进行数据恢复，先做基于schema的数据备份，然后drop当前用户，再新建用户，再导入数据。 如果用户名、表空间名称不一致，可以使用REMAP\_SCHEMA、REMAP\_TABLESPACE选择项进行映射）
7. SQL注入验证：针对实验三开发的应用程序，验证SQL注入，并提供相应的解决方案，预防SQL注入；要求至少验证2个不同的SQL注入场景。给出测试场景、测试过程、测试结果、预防方案与实际结果。
8. 实验总结与建议：针对本学期的课程实验，做实验总结（如收获、经验或不足等），并对本实验课程给出相应的意见或者建议。