

# 数据库系统及安全

## 实验手册

学号：20373108

姓名：张耀东

网络空间安全学院

2022 年秋季

## 实验四、数据库系统安全实验

### 一、实验目的

- 1、熟悉与掌握数据库安全的基本概念和技术；
- 2、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；
- 3、了解数据库管理系统安全加固的基本方法；
- 4、掌握数据库备份与恢复的基本方法；
- 5、了解 SQL 注入的基本原理和预防方法。

### 二、实验要求

- 1、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。
- 2、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。
- 3、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
- 4、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。

### 三、实验内容

1、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）

创建名为 user1 的用户，	create user user1 identified by user1;
-----------------	--

密码为 user1	
赋予 user1 登录和访问表空间的权限	<pre>grant create session to user1; grant unlimited tablespace to user1;</pre>
根据实验 3 实际情况, 授权用户 (包括管理员用户) 对三张表格进行查询、插入、更新操作。	<pre>grant select on Students to user1; grant select on Classifications to user1; grant select on Borrows to user1; grant select on Books to user1; grant insert on Students to user1; grant insert on Classifications to user1; grant insert on Borrows to user1; grant insert on Books to user1; grant update on Students to user1; grant update on Classifications to user1; grant update on Borrows to user1; grant update on Books to user1;</pre>
SQL 脚本截图	 <p>The screenshot shows a code editor with a dark background. The file name is 'ex1.sql'. The path is 'D: &gt; buaa &gt; 大3上 &gt; 数据库系统及安全实验 &gt; 实验4 &gt; ex1.sql'. The script contains 18 lines of SQL commands, which are identical to the ones listed in the previous row of the table.</p> <pre>1 create user user1 identified by user1; 2 3 grant create session to user1; 4 grant unlimited tablespace to user1; 5 6 grant select on Students to user1; 7 grant select on Classifications to user1; 8 grant select on Borrows to user1; 9 grant select on Books to user1; 10 grant insert on Students to user1; 11 grant insert on Classifications to user1; 12 grant insert on Borrows to user1; 13 grant insert on Books to user1; 14 grant update on Students to user1; 15 grant update on Classifications to user1; 16 grant update on Borrows to user1; 17 grant update on Books to user1; 18</pre>

授权截图	<pre>SQL&gt; @ex1.sql 用户已创建。  授权成功。  授权成功。  授权成功。  授权成功。  授权成功。  授权成功。  授权成功。  授权成功。  授权成功。  授权成功。  授权成功。  授权成功。  授权成功。  授权成功。  SQL&gt;</pre>
权限验证截图	<pre>D:\BUAA\大3上\数据库系统及安全实验\实验4&gt;sqlplus user1/user1@xepdb1  SQL*Plus: Release 21.0.0.0.0 - Production on 星期一 12月 12 02:10:07 2022 Version 21.3.0.0.0  Copyright (c) 1982, 2021, Oracle. All rights reserved.  连接到: Oracle Database 21c Express Edition Release 21.0.0.0.0 - Production Version 21.3.0.0.0  SQL&gt; select * from ot.students where sno='20370001';  SNO ----- NAME ----- PASSWORD_HASH TELEPHONE HOLD      ROLE ----- 20370001 测试用户 098f6bcd4621d373cade4e832627b4f6 0          0          12345678912</pre>
权限受限验证	<pre>SQL&gt; create table MyStudents(   2  Msno NUMBER GENERATED BY DEFAULT AS IDENTITY,   3  Msname VARCHAR(10),   4  PRIMARY KEY(Msno)   5  ); create table MyStudents( * 第 1 行出现错误: ORA-01031: 权限不足</pre>

2、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。

方案设计	利用已有的加解密工具，实现本地对用户名和密码的加解密。在配置文件里填写用户名与密码的密文，并写好接口，使得在登录数据库时将密文传输到本地加解密应用程序，经过个人确认来对传来的密文（用户名和密码的密文）后进行解密然后回传，从而连接数据库。
现有方案	<p>加密工具:Druid中的工具类 com.alibaba.druid.filter.config.ConfigTools, 使用其中的 encrypt(String plainText)方法和 decrypt(String cipherText)方法采用默认的公私钥加解密。</p> <p>加密文件配置:</p> <pre>1 connection.url=jdbc:mysql://127.0.0.1:3306/test 2 connection.username=*****加密后的用户名***** 3 connection.password=*****加密后的密码*****</pre> <p>重写用户名和密码的方法为解密后端登录时传入的数据:</p> <pre>1 import com.alibaba.druid.filter.config.ConfigTools; 2 import com.alibaba.druid.pool.DruidDataSource; 3 4 public class SecurityDataSource extends DruidDataSource{ 5     @Override 6     public void setUsername(String username) { 7         try { 8             username = ConfigTools.decrypt(username); 9         } catch (Exception e) { 10             e.printStackTrace(); 11         } 12         super.setUsername(username); 13     } 14 15     @Override 16     public void setPassword(String password) { 17         try { 18             password = ConfigTools.decrypt(password); 19         } catch (Exception e) { 20             e.printStackTrace(); 21         } 22         super.setPassword(password); 23     } 24 25     public static void main(String[] args) throws Exception{ 26         String password = "root"; 27         String username = "root"; 28         System.out.println("加密后的password = [" + ConfigTools.encrypt(password) + "]"); 29         System.out.println("加密后的username = [" + ConfigTools.encrypt(username) + "]"); 30     } 31 }</pre> <p>在 Spring 文件中配置数据源:</p> <pre>&lt;bean id="dataSource" class="com.wei.core.database.SecurityDataSource" init-method="init" destroy-method="close"&gt;   &lt;property name="url" value="\${jdbc.url}" /&gt;   &lt;property name="username" value="\${jdbc.username}" /&gt;   &lt;property name="password" value="\${jdbc.password}" /&gt; &lt;/bean&gt;</pre> <p>由此重写了后端登录接口处的输入。</p>

3、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。

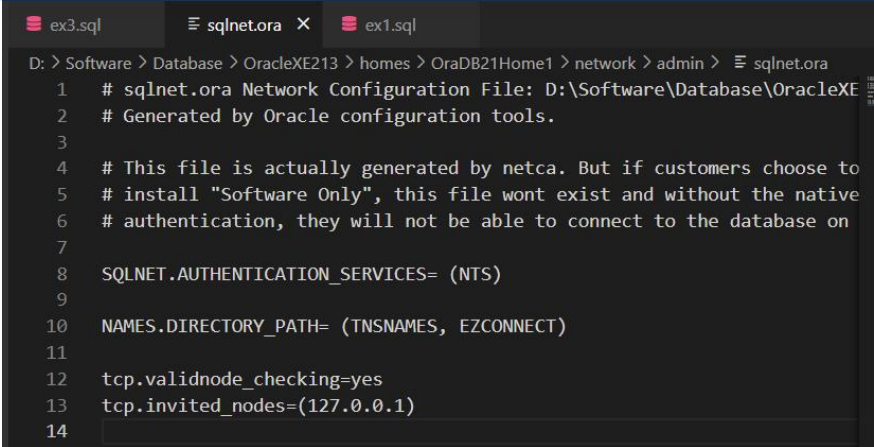
<p>1.将&lt;oracle 安装路径 \\homes\\OraDB21Home1\\network\\admin\\sqlnet.ora&gt;文件中 SQLNET.AUTHENTICATION_SERVICES= (NTS)行进行注释，即设置为口 令文件认证模式：oracle 认为操作系统是不可靠的，若要访问数据库，必须要输入用户密码，不可以 dba 直接登录数据库。</p>	<pre>C:\Users\Komorebi&gt;sqlplus / as sysdba  SQL*Plus: Release 21.0.0.0.0 - Production on 星期一 12月 12 03:03:58 2022 Version 21.3.0.0.0  Copyright (c) 1982, 2021, Oracle. All rights reserved.  连接到: Oracle Database 21c Express Edition Release 21.0.0.0.0 - Production Version 21.3.0.0.0  SQL&gt;</pre>  <pre>C:\Users\Komorebi&gt;sqlplus / as sysdba  SQL*Plus: Release 21.0.0.0.0 - Production on 星期一 12月 12 03:00:44 2022 Version 21.3.0.0.0  Copyright (c) 1982, 2021, Oracle. All rights reserved.  ERROR: ORA-01017: 用户名/口令无效; 登录被拒绝  请输入用户名: _</pre>
---	--

2. 首先创建 profile, 对资源进行限定, 然后创建用户, 将 profile 应用于用户 User1

```
ex3.sql  ex3_bk.sql X  ex1.sql
D: > buaa > 大3上 > 数据库系统及安全实验 > 实验4 > ex3_bk.sql
1  -- 创建profile
2  create profile test_profile limit
3  -- 限制用户密码的复杂度
4  password_verify_function ora12c_verify_function
5  -- 指定同一密码所允许使用的天数。
6  password_life_time 60
7  -- 指定宽限天数, 数据库发出警告到登陆失效前的天数。
8  password_grace_time 10
9  -- 指定在帐户被锁定之前所允许尝试登陆的的最大次数。
10 failed_login_attempts 3
11 -- 指定登陆尝试失败次数到达后帐户的锁定时间, 以天为单位。
12 password_lock_time 1
13 -- 指定会话允许连续不活动的总的时间, 以分钟为单位, 超过该时间, 会话将断开。
14 idle_time 10;
15
16 -- 将配置文件分配给用户
17 alter user User1 profile test_profile;
```

其中, 口令复杂度验证如下:



	<pre>SQL&gt; alter user user1 identified by User1 replace user1; alter user user1 identified by User1 replace user1 * 第 1 行出现错误: ORA-28003: 指定口令的口令验证失败 ORA-20000: password length less than 8 characters  SQL&gt; alter user user1 identified by User111111 replace user; alter user user1 identified by User111111 replace user * 第 1 行出现错误: ORA-28008: 无效的旧口令  SQL&gt; alter user user1 identified by User111111 replace user1; alter user user1 identified by User111111 replace user1 * 第 1 行出现错误: ORA-28003: 指定口令的口令验证失败 ORA-20000: password must contain 1 or more special characters  SQL&gt; alter user user1 identified by User11_ replace user1; alter user user1 identified by User11_ replace user1 * 第 1 行出现错误: ORA-28003: 指定口令的口令验证失败 ORA-20000: password length less than 8 characters  SQL&gt; alter user user1 identified by User11_23 replace user1; alter user user1 identified by User11_23 replace user1 * 第 1 行出现错误: ORA-28003: 指定口令的口令验证失败 ORA-20000: 口令包含用户名  SQL&gt; alter user user1 identified by U_ser11_23 replace user1; 用户已更改。  SQL&gt;</pre>
<p>3.将&lt;oracle 安装 路径 \\homes\\OraDB21 Home1\\network\\a dmin\\sqlnet.ora&gt; 添加最后两行: &lt;tcp.validnode_c hecking=yes&gt; (开 启 ip 限制功能), &lt;tcp.invited_node</p>	 <pre>ex3.sql  sqlnet.ora  ex1.sql D: &gt; Software &gt; Database &gt; OracleXE213 &gt; homes &gt; OraDB21Home1 &gt; network &gt; admin &gt; sqlnet.ora 1  # sqlnet.ora Network Configuration File: D:\Software\Database\OracleXE 2  # Generated by Oracle configuration tools. 3 4  # This file is actually generated by netca. But if customers choose to 5  # install "Software Only", this file wont exist and without the native 6  # authentication, they will not be able to connect to the database on 7 8  SQLNET.AUTHENTICATION_SERVICES= (NTS) 9 10 NAMES.DIRECTORY_PATH= (TNSNAMES, EZCONNECT) 11 12 tcp.validnode_checking=yes 13 tcp.invited_nodes=(127.0.0.1) 14</pre>



s=(127.0.0.1)> (只允许 127.0.0.1 的 ip 访 问)	
--	--

4、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）

指令	<pre>-- 到 xepdb1 会话中 alter session set container = xepdb1; -- 创建用户 create user OT identified by ot; -- 赋予用户权限 GRANT CONNECT, RESOURCE, DBA TO OT; -- 导入初始数据 @./oracle_sql/schema_oracle.sql; @./oracle_sql/data_oracle.sql;  -- 创建 directory 对象 create directory backup as 'D:\TmpFile\db_bk\';  -- drop directory backup;  -- 将当前目录的权限授予 grant read,write on directory backup to public;  -- 退出 exit;  -- 以下在命令行（cmd）中执行  -- 导出 expdp OT/ot@xepdb1 tables = Students job_name=ex4_data1 directory=backup parallel=1 dumpfile=Students.dmp content=all logfile=ex4_data1.log expdp OT/ot@xepdb1 tables = Classifications job_name=ex4_data4 directory=backup parallel=1 dumpfile=Classifications.dmp content=all logfile=ex4_data4.log expdp OT/ot@xepdb1 tables = Books job_name=ex4_data2 directory=backup parallel=1 dumpfile=Books.dmp content=all logfile=ex4_data2.log expdp OT/ot@xepdb1 tables = Borrows job_name=ex4_data3 directory=backup</pre>
----	--

	<pre>parallel=1 dumpfile=Borrows.dmp content=all logfile=ex4_data3.log  -- 到 xepdb1 会话中 alter session set container = xepdb1;  -- 删除用户 drop user OT CASCADE;  -- 创建新用户 create user ot_bk identified by ot_bk;  -- drop user ot_bk CASCADE; -- 赋予新用户权限 GRANT CONNECT, RESOURCE, DBA TO ot_bk;  -- 导入 impdp ot_bk/ot_bk@xepdb1 tables="OT"."STUDENTS" directory=backup dumpfile=Students.dmp REMAP_SCHEMA=OT:ot_bk REMAP_TABLESPACE=OT:ot_bk impdp ot_bk/ot_bk@xepdb1 tables="OT"."Classifications" directory=backup dumpfile=Classifications.dmp REMAP_SCHEMA=OT:ot_bk REMAP_TABLESPACE=OT:ot_bk impdp ot_bk/ot_bk@xepdb1 tables="OT"."Books" directory=backup dumpfile=Books.dmp REMAP_SCHEMA=OT:ot_bk REMAP_TABLESPACE=OT:ot_bk impdp ot_bk/ot_bk@xepdb1 tables="OT"."Borrows" directory=backup dumpfile=Borrows.dmp REMAP_SCHEMA=OT:ot_bk REMAP_TABLESPACE=OT:ot_bk</pre>
截图 验证	<p>首先在 xepdb1 下创建 OT 并授权，并建立四张表（schema 为默认） 然后创建目录，名为 backup，并对公共开放（或者分别对 OT 和之后建立的 ot_bk 开放，这里简写为 public）：</p> <pre>SQL&gt; create directory backup as 'D:\TmpFile\db_bk'; 目录已创建。  SQL&gt; grant read,write on directory backup to public; 授权成功。</pre> <p>输入上述指令进行备份并导出：</p> <pre>D:\buaa\大3上\数据库系统及安全实验\实验4\expdp OT/ot@xepdb1 tables = Students job_name=ex4_data1 directory=backup parallel=1 dumpfile=Students.dmp content=all logfile=ex4_data1.log Export: Release 21.0.0.0.0 - Production on 星期一 12月 12 23:25:37 2022 Version 21.3.0.0.0  Copyright (c) 1982, 2021, Oracle and/or its affiliates. All rights reserved.  连接到: Oracle Database 21c Express Edition Release 21.0.0.0.0 - Production 启动 "OT"."EX4_DATA1": OT/*****@xepdb1 tables=Students job_name=ex4_data1 directory=backup parallel=1 dumpfile=Students.dmp content=all logfile=ex4_data1.log 处理对象类型 TABLE_EXPORT/TABLE/TABLE_DATA 处理对象类型 TABLE_EXPORT/TABLE/INDEX/STATISTICS/INDEX_STATISTICS 处理对象类型 TABLE_EXPORT/TABLE/STATISTICS/TABLE_STATISTICS 处理对象类型 TABLE_EXPORT/TABLE/STATISTICS/MARKER 处理对象类型 TABLE_EXPORT/TABLE/TABLE 处理对象类型 TABLE_EXPORT/TABLE/CONSTRAINT/CONSTRAINT . 导出了 "OT"."STUDENTS" 9,890 KB 40 行 已成功加载/卸载了主表 "OT"."EX4_DATA1" ***** OT, EX4_DATA1 的转储文件集为: D:\TMPFILE\DB_BK\STUDENTS.DMP 作业 "OT"."EX4_DATA1" 已于 星期一 12月 12 23:25:52 2022 elapsed 0 00:00:13 成功完成</pre>

```
D:\buaa\大3上\数据库系统及安全实验\实验4\expdp OT\ot@expdb1 tables = Classifications job_name=ex4_data4 directory=backup parallel=1 dumpfile=Classifications.dmp content=all logfile=ex4_data4.log
Export: Release 21.0.0.0.0 - Production on 星期一 12月 12 23:27:05 2022
Version 21.3.0.0.0

Copyright (c) 1982, 2021, Oracle and/or its affiliates. All rights reserved.

连接到: Oracle Database 21c Express Edition Release 21.0.0.0.0 - Production
启动 "OT"."EX4_DATA4": OT/*****@expdb1 tables=Classifications job_name=ex4_data4 directory=backup parallel=1 dumpfile=Classifications.dmp content=all logfile=ex4_data4.log
处理对象类型 TABLE EXPORT/TABLE/TABLE DATA
处理对象类型 TABLE EXPORT/TABLE/INDEX/STATISTICS/INDEX_STATISTICS
处理对象类型 TABLE EXPORT/TABLE/STATISTICS/TABLE_STATISTICS
处理对象类型 TABLE EXPORT/TABLE/STATISTICS/MARKER
处理对象类型 TABLE EXPORT/TABLE/TABLE
处理对象类型 TABLE EXPORT/TABLE/IDENTITY COLUMN
处理对象类型 TABLE EXPORT/TABLE/CONSTRAINT/CONSTRAINT
导出 "OT"."CLASSIFICATIONS" 6,320 KB 22 行
已成功加载/卸载了主表 "OT"."EX4_DATA4"
*****
OT, EX4_DATA4 的转储文件名为:
D:\TMPFILE\DB_BK\CLASSIFICATIONS.DMP
作业 "OT"."EX4_DATA4" 已于 星期一 12月 12 23:27:19 2022 elapsed 0 00:00:12 成功完成
```

```
D:\buaa\大3上\数据库系统及安全实验\实验4\expdp OT\ot@expdb1 tables = Books job_name=ex4_data2 directory=backup parallel=1 dumpfile=Books.dmp content=all logfile=ex4_data2.log
Export: Release 21.0.0.0.0 - Production on 星期一 12月 12 23:27:38 2022
Version 21.3.0.0.0

Copyright (c) 1982, 2021, Oracle and/or its affiliates. All rights reserved.

连接到: Oracle Database 21c Express Edition Release 21.0.0.0.0 - Production
启动 "OT"."EX4_DATA2": OT/*****@expdb1 tables=Books job_name=ex4_data2 directory=backup parallel=1 dumpfile=Books.dmp content=all logfile=ex4_data2.log
处理对象类型 TABLE EXPORT/TABLE/TABLE DATA
处理对象类型 TABLE EXPORT/TABLE/INDEX/STATISTICS/INDEX_STATISTICS
处理对象类型 TABLE EXPORT/TABLE/STATISTICS/TABLE_STATISTICS
处理对象类型 TABLE EXPORT/TABLE/STATISTICS/MARKER
处理对象类型 TABLE EXPORT/TABLE/TABLE
处理对象类型 TABLE EXPORT/TABLE/CONSTRAINT/CONSTRAINT
处理对象类型 TABLE EXPORT/TABLE/CONSTRAINT/REF_CONSTRAINT
导出 "OT"."BOOKS" 13.53 KB 102 行
已成功加载/卸载了主表 "OT"."EX4_DATA2"
*****
OT, EX4_DATA2 的转储文件名为:
D:\TMPFILE\DB_BK\BOOKS.DMP
作业 "OT"."EX4_DATA2" 已于 星期一 12月 12 23:27:52 2022 elapsed 0 00:00:12 成功完成
```

```
D:\buaa\大3上\数据库系统及安全实验\实验4\expdp OT\ot@expdb1 tables = Borrows job_name=ex4_data3 directory=backup parallel=1 dumpfile=Borrows.dmp content=all logfile=ex4_data3.log
Export: Release 21.0.0.0.0 - Production on 星期一 12月 12 23:28:25 2022
Version 21.3.0.0.0

Copyright (c) 1982, 2021, Oracle and/or its affiliates. All rights reserved.

连接到: Oracle Database 21c Express Edition Release 21.0.0.0.0 - Production
启动 "OT"."EX4_DATA3": OT/*****@expdb1 tables=Borrows job_name=ex4_data3 directory=backup parallel=1 dumpfile=Borrows.dmp content=all logfile=ex4_data3.log
处理对象类型 TABLE EXPORT/TABLE/TABLE DATA
处理对象类型 TABLE EXPORT/TABLE/INDEX/STATISTICS/INDEX_STATISTICS
处理对象类型 TABLE EXPORT/TABLE/STATISTICS/TABLE_STATISTICS
处理对象类型 TABLE EXPORT/TABLE/STATISTICS/MARKER
处理对象类型 TABLE EXPORT/TABLE/TABLE
处理对象类型 TABLE EXPORT/TABLE/IDENTITY COLUMN
处理对象类型 TABLE EXPORT/TABLE/CONSTRAINT/CONSTRAINT
处理对象类型 TABLE EXPORT/TABLE/CONSTRAINT/REF_CONSTRAINT
导出 "OT"."BORROWS" 7.437 KB 18 行
已成功加载/卸载了主表 "OT"."EX4_DATA3"
*****
OT, EX4_DATA3 的转储文件名为:
D:\TMPFILE\DB_BK\BORROWS.DMP
作业 "OT"."EX4_DATA3" 已于 星期一 12月 12 23:28:39 2022 elapsed 0 00:00:12 成功完成
```

backup 所在文件下导出后显示:

BOOKS.DMP	2022/12/12 23:27	DMP 文件	216 KB
BORROWS.DMP	2022/12/12 23:28	DMP 文件	216 KB
CLASSIFICATIONS.DMP	2022/12/12 23:27	DMP 文件	200 KB
ex4_data1.log	2022/12/12 23:25	文本文档	2 KB
ex4_data2.log	2022/12/12 23:27	文本文档	2 KB
ex4_data3.log	2022/12/12 23:28	文本文档	2 KB
ex4_data4.log	2022/12/12 23:27	文本文档	2 KB
import.log	2022/12/12 23:38	文本文档	2 KB
STUDENTS.DMP	2022/12/12 23:25	DMP 文件	204 KB

在 sysdba 视角下删除 OT，并建立新的用户 ot\_bk:

```
SQL> drop user OT CASCADE;

用户已删除。

SQL> create user ot_bk identified by ot_bk;

用户已创建。

SQL> GRANT CONNECT, RESOURCE, DBA TO ot_bk;

授权成功。
```

## 利用 ot\_bk 身份导出数据库内的表（默认 schema）：

```
D:\buaa\大3上\数据库系统及安全实验\实验4\impdp ot_bk\ot_bk@xepdb1 tables="OT"."STUDENTS" directory=backup dumpfile=Students.dmp REMAP_SCHEMA=OT:ot_bk REMAP_TABLESPACE=OT:ot_bk
Import: Release 21.0.0.0.0 - Production on 星期一 - 12月 12 23:35:32 2022
Version 21.3.0.0.0

Copyright (c) 1982, 2021, Oracle and/or its affiliates. All rights reserved.

连接到: Oracle Database 21c Express Edition Release 21.0.0.0.0 - Production
已成功加载/卸载了主表 "OT_BK"."SYS_IMPORT_TABLE_01"
启动 "OT_BK"."SYS_IMPORT_TABLE_01": ot_bk/*****@xepdb1 tables=OT.STUDENTS directory=backup dumpfile=Students.dmp REMAP_SCHEMA=OT:ot_bk REMAP_TABLESPACE=OT:ot_bk
处理对象类型 TABLE EXPORT/TABLE/TABLE
处理对象类型 TABLE EXPORT/TABLE/TABLE_DATA
. 导入了 "OT_BK"."STUDENTS" 9.890 KB 40 行
处理对象类型 TABLE EXPORT/TABLE/CONSTRAINT/CONSTRAINT
处理对象类型 TABLE EXPORT/TABLE/INDEX/STATISTICS/INDEX STATISTICS
处理对象类型 TABLE EXPORT/TABLE/STATISTICS/TABLE_STATISTICS
处理对象类型 TABLE EXPORT/TABLE/STATISTICS/MARKER
作业 "OT_BK"."SYS_IMPORT_TABLE_01" 已于 星期一 - 12月 12 23:35:47 2022 elapsed 0 00:00:13 成功完成
```

```
D:\buaa\大3上\数据库系统及安全实验\实验4\impdp ot_bk\ot_bk@xepdb1 tables="OT"."Classifications" directory=backup dumpfile=Classifications.dmp REMAP_SCHEMA=OT:ot_bk REMAP_TABLESPACE=OT:ot_bk
Import: Release 21.0.0.0.0 - Production on 星期一 - 12月 12 23:37:10 2022
Version 21.3.0.0.0

Copyright (c) 1982, 2021, Oracle and/or its affiliates. All rights reserved.

连接到: Oracle Database 21c Express Edition Release 21.0.0.0.0 - Production
已成功加载/卸载了主表 "OT_BK"."SYS_IMPORT_TABLE_01"
启动 "OT_BK"."SYS_IMPORT_TABLE_01": ot_bk/*****@xepdb1 tables=OT.Classifications directory=backup dumpfile=Classifications.dmp REMAP_SCHEMA=OT:ot_bk REMAP_TABLESPACE=OT:ot_bk
处理对象类型 TABLE EXPORT/TABLE/TABLE
处理对象类型 TABLE EXPORT/TABLE/TABLE_DATA
. 导入了 "OT_BK"."CLASSIFICATIONS" 6.320 KB 22 行
处理对象类型 TABLE EXPORT/TABLE/IDENTITY COLUMN
处理对象类型 TABLE EXPORT/TABLE/CONSTRAINT/CONSTRAINT
处理对象类型 TABLE EXPORT/TABLE/INDEX/STATISTICS/INDEX STATISTICS
处理对象类型 TABLE EXPORT/TABLE/STATISTICS/TABLE_STATISTICS
处理对象类型 TABLE EXPORT/TABLE/STATISTICS/MARKER
作业 "OT_BK"."SYS_IMPORT_TABLE_01" 已于 星期一 - 12月 12 23:37:26 2022 elapsed 0 00:00:14 成功完成
```

```
D:\buaa\大3上\数据库系统及安全实验\实验4\impdp ot_bk\ot_bk@xepdb1 tables="OT"."Books" directory=backup dumpfile=Books.dmp REMAP_SCHEMA=OT:ot_bk REMAP_TABLESPACE=OT:ot_bk
Import: Release 21.0.0.0.0 - Production on 星期一 - 12月 12 23:37:44 2022
Version 21.3.0.0.0

Copyright (c) 1982, 2021, Oracle and/or its affiliates. All rights reserved.

连接到: Oracle Database 21c Express Edition Release 21.0.0.0.0 - Production
已成功加载/卸载了主表 "OT_BK"."SYS_IMPORT_TABLE_01"
启动 "OT_BK"."SYS_IMPORT_TABLE_01": ot_bk/*****@xepdb1 tables=OT.Books directory=backup dumpfile=Books.dmp REMAP_SCHEMA=OT:ot_bk REMAP_TABLESPACE=OT:ot_bk
处理对象类型 TABLE EXPORT/TABLE/TABLE
处理对象类型 TABLE EXPORT/TABLE/TABLE_DATA
. 导入了 "OT_BK"."BOOKS" 13.53 KB 102 行
处理对象类型 TABLE EXPORT/TABLE/CONSTRAINT/CONSTRAINT
处理对象类型 TABLE EXPORT/TABLE/INDEX/STATISTICS/INDEX STATISTICS
处理对象类型 TABLE EXPORT/TABLE/CONSTRAINT/REF CONSTRAINT
处理对象类型 TABLE EXPORT/TABLE/STATISTICS/TABLE_STATISTICS
处理对象类型 TABLE EXPORT/TABLE/STATISTICS/MARKER
作业 "OT_BK"."SYS_IMPORT_TABLE_01" 已于 星期一 - 12月 12 23:38:00 2022 elapsed 0 00:00:14 成功完成
```

```
D:\buaa\大3上\数据库系统及安全实验\实验4\impdp ot_bk\ot_bk@xepdb1 tables="OT"."Borrows" directory=backup dumpfile=Borrows.dmp REMAP_SCHEMA=OT:ot_bk REMAP_TABLESPACE=OT:ot_bk
Import: Release 21.0.0.0.0 - Production on 星期一 - 12月 12 23:38:19 2022
Version 21.3.0.0.0

Copyright (c) 1982, 2021, Oracle and/or its affiliates. All rights reserved.

连接到: Oracle Database 21c Express Edition Release 21.0.0.0.0 - Production
已成功加载/卸载了主表 "OT_BK"."SYS_IMPORT_TABLE_01"
启动 "OT_BK"."SYS_IMPORT_TABLE_01": ot_bk/*****@xepdb1 tables=OT.Borrows directory=backup dumpfile=Borrows.dmp REMAP_SCHEMA=OT:ot_bk REMAP_TABLESPACE=OT:ot_bk
处理对象类型 TABLE EXPORT/TABLE/TABLE
处理对象类型 TABLE EXPORT/TABLE/TABLE_DATA
. 导入了 "OT_BK"."BORROWS" 7.437 KB 18 行
处理对象类型 TABLE EXPORT/TABLE/IDENTITY COLUMN
处理对象类型 TABLE EXPORT/TABLE/CONSTRAINT/CONSTRAINT
处理对象类型 TABLE EXPORT/TABLE/INDEX/STATISTICS/INDEX STATISTICS
处理对象类型 TABLE EXPORT/TABLE/CONSTRAINT/REF CONSTRAINT
处理对象类型 TABLE EXPORT/TABLE/STATISTICS/TABLE_STATISTICS
处理对象类型 TABLE EXPORT/TABLE/STATISTICS/MARKER
作业 "OT_BK"."SYS_IMPORT_TABLE_01" 已于 星期一 - 12月 12 23:38:34 2022 elapsed 0 00:00:13 成功完成
```

## 验证导出数据库是否可用：

```
D:\buaa\大3上\数据库系统与安全实验\实验4>sqlplus ot_bk/ot_bk@xepdb1

SQL*Plus: Release 21.0.0.0.0 - Production on 星期一 12月 12 23:43:41 2022
Version 21.3.0.0.0

Copyright (c) 1982, 2021, Oracle. All rights reserved.

上次成功登录时间: 星期一 12月 12 2022 23:43:07 +08:00

连接到:
Oracle Database 21c Express Edition Release 21.0.0.0.0 - Production
Version 21.3.0.0.0

SQL> select * from students where sno = '20373108';

SNO
-----
NAME
-----
PASSWORD_HASH                                TELEPHONE
-----
HOLD      ROLE
-----
20373108
张耀东
ba157d2ecdcaeac516b27cf02bf45e59          13349184119
0      1
```

5、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。

在实验三中对 sql 注入已有防备，主要利用？进行传参操作，？默认对参数进行编码，具有防止 sql 注入的功能，仅有的三处使用\${}进行传参的功能分别在书籍查询（所有人）、借阅记录查询（管理员）、修改书名（管理员）处，皆是由于为了使用模糊比较而寻求方便才使用而\${}。下面针对前两处进行讨论，并给出两种解决方案。

注入场景一：在图书搜索栏中 sql 语句为<SELECT books.book\_name,books.author\_name,books.ISBN,classifications.classification,classifications.location,books.current,books.total FROM books,classifications WHERE books.classification = classifications.id AND books.book\_name LIKE '%\$\${data.info}%'>,利用\${}进行传参

解决方案：利用 mysql.escape（）对传入参数进行编码，防止篡改 sql 语句使其发挥其他作用。

```
...e LIKE ${mysql.escape("%"+data.info+"%")};~;
...ame LIKE ${mysql.escape("%"+data.info+"%")};~;
```

修改后语句为<SELECT books.book\_name,books.author\_name,books.ISBN,classifications.classification,classifications.location,books.current,books.total FROM



（将传入的数据直接显示生成在 sql 语句中），使得可以导入适当的 sql 语句使得执行结果不同，如：<冯%' union SELECT books.book\_name,books.author\_name,books.ISBN,classifications.classification,classifications.location,books.current,books.total FROM books,classifications WHERE books.classification = classifications.id AND books.book\_name LIKE '%老人与海> 查询结果包含了“冯”与“老人与海”两个关键词

冯%' union SELECT books.book_name,books.author_name,books.ISBN						搜索
图书名称	图书作者	ISBN	分类	当前可借阅	操作	
> 冯骥才游手札-游手札-全彩图文版	冯骥才	9787535494184	文化	275	借阅	
> 《老人与海》	海明威	9787506385831	文学	240	借阅	
> 俗世奇人-贰	冯骥才	9787108050434	文学	113	借阅	
> 《爱情是一盘自制卡带》	[美]谢菲尔 德 著, 冯 儒珠 译	9787305111341	文学	200	借阅	
> 《一种人生观》	冯友兰	9787516831953	文学	135	借阅	

同理，可以利用 sql 注入在没有管理员权限的情况下查询其他用户信息

注入场景二：在查询借阅记录中使用规定 sql 语句为<SELECT borrows.id,students.Sno,students.name,books.book\_name,books.author\_name,books.ISBN,borrows.borrow\_date,DATE\_ADD(borrows.borrow\_date,INTERVAL 30

```
books,classifications WHERE books.classification = classifications.id AND books.book_name LIKE ${mysql.escape("%"+data.info+"%")} } ;>
```

修改输入尝试 sql 注入：<冯%' union SELECT books.book\_name,books.author\_name,books.ISBN,classifications.classification,classifications.location,books.current,books.total FROM books,classifications WHERE books.classification = classifications.id AND books.book\_name LIKE '%老人与海>

注入结果：



解决方案：利用?引入参数会使得引入值进行编码，防止篡改 sql 语句使其发挥其他作用。

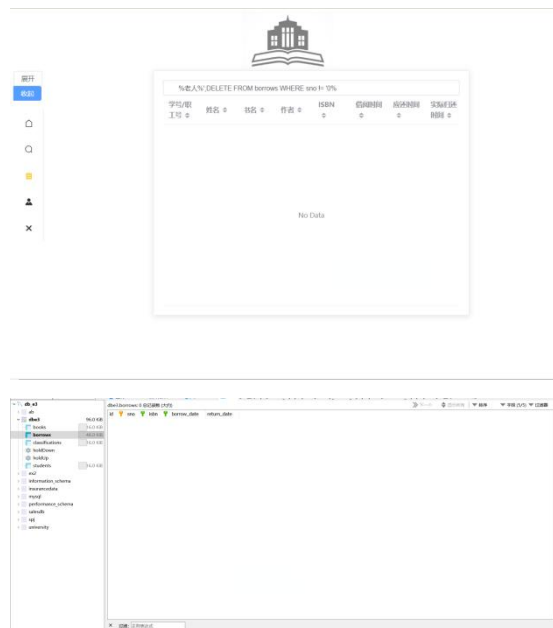
```
WHERE borrows.Sno=students.Sno AND borrows.ISBN=books.ISBN AND books.book_name LIKE ?";
```

修改后语句为<SELECT borrows.id,students.Sno,students.n



```
day) date_time, borrows.return_date,
if (borrows.return_date IS NULL, '未
还', '已还') status FROM
borrows, students, books WHERE
borrows.Sno=students.Sno AND
borrows.ISBN=books.ISBN AND
books.book_name LIKE
'%${data.info}%';>
```

设置输入参数为<老人%';DELETE FROM  
borrows WHERE sno != '0>



数据库已经被删除

```
ame, books.book_name, books.author_n
ame, books.ISBN, borrows.borrow_date
, DATE_ADD (borrows.borrow_date, INTE
RVAL 30
day) date_time, borrows.return_date,
if (borrows.return_date IS NULL, '未还
', '已还') status FROM
borrows, students, books WHERE
borrows.Sno=students.Sno AND
borrows.ISBN=books.ISBN AND
books.book_name LIKE ?;>
```

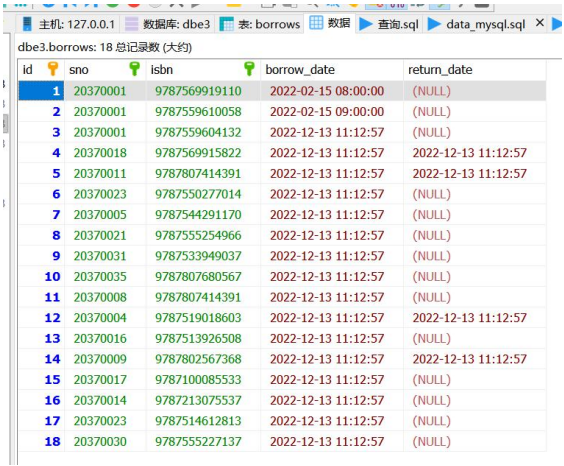
修改输入尝试 sql 注入: <老人%';DELETE  
FROM borrows WHERE sno != '0>

注入结果: 失败



刷新后:

请输入您要查找的用户学号/职工号/图书名称							
学号/职工号	姓名	书名	作者	ISBN	借阅时间	应还时间	实际归还时间
20370001	测试用户	呼兰河传	萧红	9787569919110	2022-02-15 08:00:00	2022-03-17 08:00:00	
20370001	测试用户	《瓦尔登湖》	[美]亨利·戴维·梭罗著, 肖篱译	9787559610058	2022-02-15 09:00:00	2022-03-17 09:00:00	
20370001	测试用户	今生要云的100个中国5A景区	赖娟燕	9787559604132	2022-12-13 11:25:57	2023-01-12 11:25:57	
20370018	方君彦	《官墙里: 一个人的乡村》	阎海军	9787569915822	2022-12-13 11:25:57	2023-01-12 11:25:57	2022-12-13 11:25:57

	数据库内显示:
	

6、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。

答：本学期通过数据库实验能够加深我对老师上课传授的知识理解，并且切实学到许许多多的东西。如从第一节课开始对 oracle 比较陌生，到第二节课可以较为熟练地进行增删改查数据，建立用户和表等等。在第三节课，更是促使我学习了网页前后端的开发以及后端与数据库的连接。在这第四节课切实主题，交了许多关于数据库安全的东西，也让我学会了许许多多重要的知识点，让我意识到之前写的系统虽然功能完备，但是在安全方面很可能因为 sql 注入而遭受入侵，或者后端对数据库端进行连接时的配置文件使用明文更是十分危险。当然数据库实验还锻炼了我的能力：根据下发的资料和网络，理解并实现需要的功能，其中由于 oracle 版本不同经常会出现许许多多意想不到的问题。以这次实验为例（这次试验印象还很深刻），在进行数据库备份和导入时，即使使用了 REMAP\_TABLESPACE 与 REMAP\_SCHEMA 也依旧显示操作错误，无法找到对象，从网上找到的指令写法并无太大差异，最后翻阅 backup 中的数据导出 log 中发现是因为命名规范的不同：导出的 table 默认为"OT"."table"（原用户名：OT，表名：table），网上的写法一般为 OT.table 或'OT.table'，而当我改为"OT"."table"时才成功。类似的示例还有很多。总之数据库实验这门课虽然学分低，但是要求并不低，我也确实在这门课中学到了许多东西。