Министерство образования и науки Российской Федерации

Федеральное государственное автономное образовательное учреждение высшего профессионального образования

**«Национальный исследовательский ядерный университет «МИФИ»**

**ИНСТИТУТ ИНТЕЛЛЕКТУАЛЬНЫХ КИБЕРНЕТИЧЕСКИХ СИСТЕМ**

**Кафедра №42 (криптологии и кибербезопасности)**

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №2-4**

«Аутентификация и базовый контроль доступа»

по дисциплине: «Безопасность систем баз данных»

**Выполнил:**  
Студент учебной группы Б19-515

Родионов Дмитрий Александрович

**Принял:**

Ассистент НИЯУ МИФИ

Куприяшин М.А.

**Москва, 2022**

**СОДЕРЖАНИЕ**

[Лист с диаграммой отношения сущностей 3](#_Toc124127899)

[Создание schema-only пользователя 4](#_Toc124127900)

[Аутентификация средствами операционной системы 7](#_Toc124127901)

[Описание разработанных представлений 8](#_Toc124127902)

[Заключение 9](#_Toc124127903)

[Приложения 10](#_Toc124127904)

# **Лист с диаграммой отношения сущностей**

Диаграмма базы данных:



# **Создание schema-only пользователя**

Организация доступа к особо важным данным:

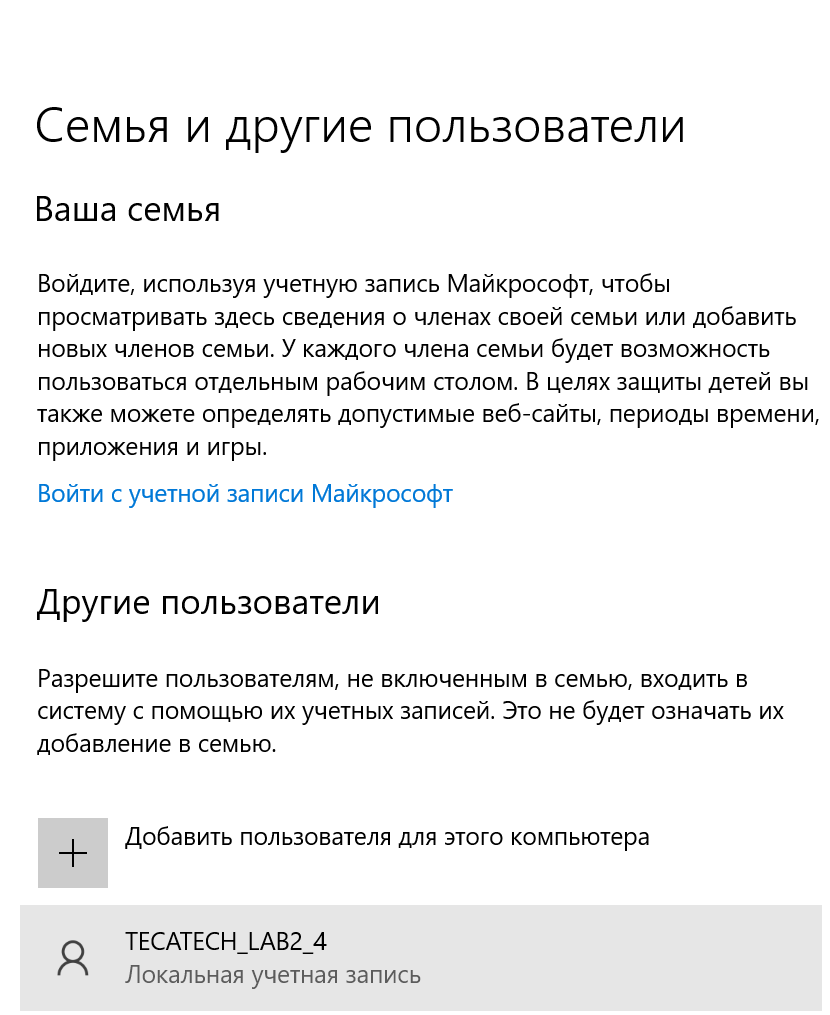
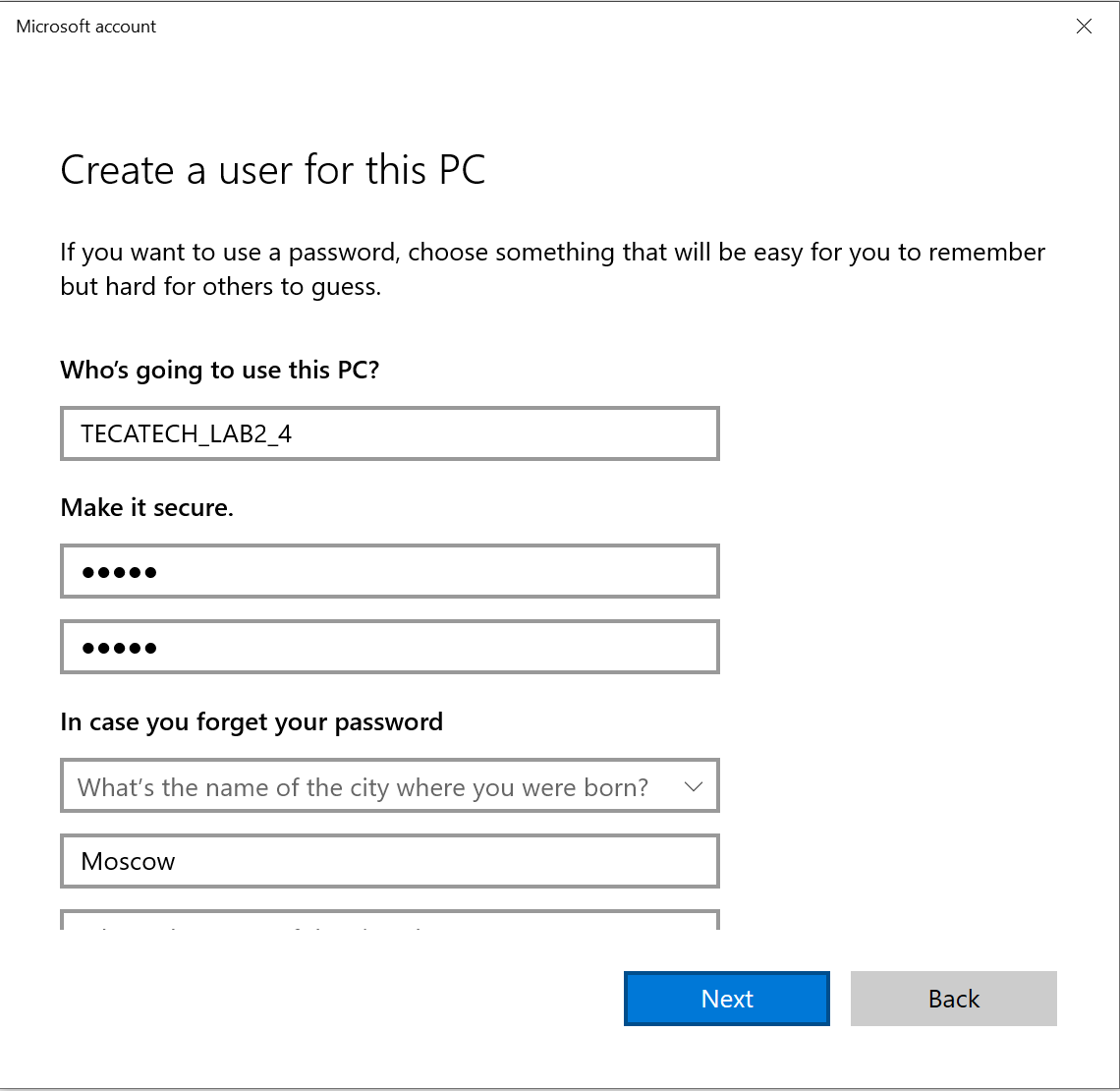
1. При управлении базой данных *хорошей* практикой является ограничение доступа к схеме посредством использования прокси-соединения. Таким образом, администратор базы данных имеет возможность проводить аудит активности пользователей, которые выполняют действия от лица владельца схемы.
2. Важно отметить, что пользователь имеет возможность подключаться напрямую к аккаунту владельца схемы. Следовательно, если аккаунт блокируется из-за превышения количества последовательных неудачных попыток входа в учетную запись, то прокси-соединение завершается неудачей.
3. В качестве решения проблемы используются schema-only пользователи, для которых при создании не задается пароль. Поскольку метод аутентификации пользователя не указывается, пользователь не имеет возможности подключаться напрямую к аккаунту владельца схемы и влиять на блокировку аккаунта. При этом администратор базы данных имеет возможность заблокировать аккаунт для ограничения прокси-соединения.
4. Если объединить все лабораторные задания по курсу дисциплины в одну работу, то в системе будут зарегистрированы и пользователи с правами администратора, и рядовые пользователи, что является основанием для использования schema-only пользователей.

Запросы к базе данных:

* CREATE USER tecatech\_lab2\_4  
   IDENTIFIED BY gamma  
   DEFAULT TABLESPACE users  
   TEMPORARY TABLESPACE temp  
   QUOTA 100M ON users;
* GRANT  
   CREATE SESSION,  
   CREATE TABLE  
  TO tecatech\_lab2\_4;
* CONNECT tecatech\_lab2\_4/gamma@"DESKTOP-UG7SO1F:1521/xepdb1";
* CREATE TABLE timestamps(  
   timestamp\_id NUMBER(4, 0) NOT NULL,  
   day NUMBER(2, 0),  
   month NUMBER(2, 0),  
   year NUMBER(4, 0),  
   PRIMARY KEY (timestamp\_id)  
  );
* GRANT  
   SELECT,  
   INSERT,  
   UPDATE,  
   DELETE  
  ON timestamps  
  TO tecatech\_lab1\_4;
* CONNECT tecatech\_lab1\_4/alpha@"DESKTOP-UG7SO1F:1521/xepdb1";
* INSERT ALL  
   INTO tecatech\_lab2\_4.timestamps(timestamp\_id, day, month, year) VALUES (1, 10, 6, 2022)  
   INTO tecatech\_lab2\_4.timestamps(timestamp\_id, day, month, year) VALUES (2, 31, 8, 2022)  
   INTO tecatech\_lab2\_4.timestamps(timestamp\_id, day, month, year) VALUES (3, 1, 1, 2023)  
   INTO tecatech\_lab2\_4.timestamps(timestamp\_id, day, month, year) VALUES (4, 31, 1, 2023)  
  SELECT \* FROM dual;
* SELECT \* FROM tecatech\_lab2\_4.timestamps;
* DROP TABLE tecatech\_lab2\_4.timestamps;
* CONNECT system/tecatech@"DESKTOP-UG7SO1F:1521/xepdb1";
* CREATE USER manager IDENTIFIED BY default;
* GRANT CREATE SESSION TO manager;
* ALTER USER tecatech\_lab2\_4 GRANT CONNECT THROUGH manager;
* CONNECT manager[tecatech\_lab2\_4]/default@"DESKTOP-UG7SO1F:1521/xepdb1";
* SELECT \* FROM timestamps;
* CONNECT system/tecatech@"DESKTOP-UG7SO1F:1521/xepdb1";
* ALTER USER tecatech\_lab2\_4 ACCOUNT LOCK;
* CONNECT manager[tecatech\_lab2\_4]/default@"DESKTOP-UG7SO1F:1521/xepdb1";
* CONNECT system/tecatech@"DESKTOP-UG7SO1F:1521/xepdb1";
* DROP USER tecatech\_lab2\_4 CASCADE;
* CREATE USER tecatech\_lab2\_4  
   NO AUTHENTICATION  
   DEFAULT TABLESPACE users  
   TEMPORARY TABLESPACE temp  
   QUOTA 100M ON users;
* GRANT  
   CREATE SESSION,  
   CREATE TABLE  
  TO tecatech\_lab2\_4;
* ALTER USER tecatech\_lab2\_4 GRANT CONNECT THROUGH manager;
* SELECT  
   username,  
   account\_status,  
   authentication\_type  
  FROM dba\_users  
  WHERE username = 'TECATECH\_LAB2\_4';
* CONNECT tecatech\_lab2\_4/gamma@"DESKTOP-UG7SO1F:1521/xepdb1";
* CONNECT manager[tecatech\_lab2\_4]/default@"DESKTOP-UG7SO1F:1521/xepdb1";
* CREATE TABLE timestamps(  
   timestamp\_id NUMBER(4, 0) NOT NULL,  
   day NUMBER(2, 0),  
   month NUMBER(2, 0),  
   year NUMBER(4, 0),  
   PRIMARY KEY (timestamp\_id)  
  );
* GRANT  
   SELECT,  
   INSERT,  
   UPDATE,  
   DELETE  
  ON timestamps  
  TO tecatech\_lab1\_4;
* CONNECT tecatech\_lab1\_4/alpha@"DESKTOP-UG7SO1F:1521/xepdb1";
* INSERT ALL  
   INTO tecatech\_lab2\_4.timestamps(timestamp\_id, day, month, year) VALUES (1, 10, 6, 2022)  
   INTO tecatech\_lab2\_4.timestamps(timestamp\_id, day, month, year) VALUES (2, 31, 8, 2022)  
   INTO tecatech\_lab2\_4.timestamps(timestamp\_id, day, month, year) VALUES (3, 1, 1, 2023)  
   INTO tecatech\_lab2\_4.timestamps(timestamp\_id, day, month, year) VALUES (4, 31, 1, 2023)  
  SELECT \* FROM dual;
* SELECT \* FROM tecatech\_lab2\_4.timestamps;
* DROP TABLE tecatech\_lab2\_4.timestamps;
* CONNECT manager[tecatech\_lab2\_4]/default@"DESKTOP-UG7SO1F:1521/xepdb1";
* SELECT \* FROM timestamps;
* CONNECT system/tecatech@"DESKTOP-UG7SO1F:1521/xepdb1";
* ALTER USER tecatech\_lab2\_4 ACCOUNT LOCK;
* CONNECT manager[tecatech\_lab2\_4]/default@"DESKTOP-UG7SO1F:1521/xepdb1";

# **Аутентификация средствами операционной системы**

Создание учетной записи Microsoft:

  
Запросы к базе данных:

* SHOW con\_name;
* SHOW PARAMETER os\_authent\_prefix;
* CREATE USER "OPS$DESKTOP-UG7SO1F\TECATECH\_LAB2\_4" IDENTIFIED EXTERNALLY;
* GRANT CREATE SESSION TO "OPS$DESKTOP-UG7SO1F\TECATECH\_LAB2\_4";
* SHOW USER;

# **Описание разработанных представлений**

Путем использования таблиц схемы создается представление:

* представление *career\_mode* определяет параметры, которые описывают ценность футболиста в режиме карьеры и являются доступными рядовому пользователю.

Запросы к базе данных:

* CREATE VIEW career\_mode AS  
   SELECT  
   players.player\_name AS player,  
   clubs.club\_name AS club,  
   national\_teams.national\_team\_name AS national\_team,  
   players.player\_ovr AS rating,  
   players.player\_age AS age  
   FROM  
   players,  
   clubs,  
   national\_teams  
   WHERE  
   players.club\_id = clubs.club\_id AND  
   players.national\_team\_id = national\_teams.national\_team\_id  
   ORDER BY  
   rating DESC,  
   age ASC;
* SELECT \* FROM career\_mode;
* GRANT CREATE SESSION TO manager;
* CREATE ROLE app\_manager\_role IDENTIFIED BY password;
* GRANT SELECT ON administrator.career\_mode TO app\_manager\_role;
* GRANT app\_manager\_role TO manager;
* CONNECT manager/default@"DESKTOP-UG7SO1F:1521/xepdb1";
* SET ROLE app\_manager\_role IDENTIFIED BY password;
* SELECT \* FROM administrator.career\_mode;
* SELECT \* FROM administrator.national\_teams;
* SELECT \* FROM administrator.leagues;
* SELECT \* FROM administrator.clubs;
* SELECT \* FROM administrator.players;

# **Заключение**

В данной лабораторной работе рассмотрены различные способы аутентификации пользователей и примитивные механизмы разграничения доступа к столбцам и записям базы данных. В частности, изучены способы аутентификации пользователей и с использованием учетных записей schema-only, и средствами операционной системы.

Также создано и применено представление, ограничивающее доступ рядовых пользователей к особо важным данным.

# **Приложения**

SQL-инструкции, использованные при создании пользователей и таблиц:

SQL> CREATE USER tecatech\_lab2\_4

2 IDENTIFIED BY gamma

3 DEFAULT TABLESPACE users

4 TEMPORARY TABLESPACE temp

5 QUOTA 100M ON users;

SQL> GRANT

2 CREATE SESSION,

3 CREATE TABLE

4 TO tecatech\_lab2\_4;

SQL> CONNECT tecatech\_lab2\_4/gamma@"DESKTOP-UG7SO1F:1521/xepdb1";

SQL> CREATE TABLE timestamps(

2 timestamp\_id NUMBER(4, 0) NOT NULL,

3 day NUMBER(2, 0),

4 month NUMBER(2, 0),

5 year NUMBER(4, 0),

6 PRIMARY KEY (timestamp\_id)

7 );

SQL> GRANT

2 SELECT,

3 INSERT,

4 UPDATE,

5 DELETE

6 ON timestamps

7 TO tecatech\_lab1\_4;

SQL> CONNECT tecatech\_lab1\_4/alpha@"DESKTOP-UG7SO1F:1521/xepdb1";

SQL> INSERT ALL

2 INTO tecatech\_lab2\_4.timestamps(timestamp\_id, day, month, year) VALUES (1, 10, 6, 2022)

3 INTO tecatech\_lab2\_4.timestamps(timestamp\_id, day, month, year) VALUES (2, 31, 8, 2022)

4 INTO tecatech\_lab2\_4.timestamps(timestamp\_id, day, month, year) VALUES (3, 1, 1, 2023)

5 INTO tecatech\_lab2\_4.timestamps(timestamp\_id, day, month, year) VALUES (4, 31, 1, 2023)

6 INTO tecatech\_lab2\_4.timestamps(timestamp\_id, day, month, year) VALUES (5, 10, 6, 2023)

7 SELECT \* FROM dual;

SQL> SELECT \* FROM tecatech\_lab2\_4.timestamps;

SQL> DROP TABLE tecatech\_lab2\_4.timestamps;

SQL> CONNECT system/tecatech@"DESKTOP-UG7SO1F:1521/xepdb1";

SQL> CREATE USER manager IDENTIFIED BY default;

SQL> GRANT CREATE SESSION TO manager;

SQL> ALTER USER tecatech\_lab2\_4 GRANT CONNECT THROUGH manager;

SQL> CONNECT manager[tecatech\_lab2\_4]/default@"DESKTOP-UG7SO1F:1521/xepdb1";

SQL> SELECT \* FROM timestamps;

SQL> CONNECT system/tecatech@"DESKTOP-UG7SO1F:1521/xepdb1";

SQL> ALTER USER tecatech\_lab2\_4 ACCOUNT LOCK;

SQL> CONNECT manager[tecatech\_lab2\_4]/default@"DESKTOP-UG7SO1F:1521/xepdb1";

SQL> CONNECT system/tecatech@"DESKTOP-UG7SO1F:1521/xepdb1";

SQL> DROP USER tecatech\_lab2\_4 CASCADE;

SQL> CREATE USER tecatech\_lab2\_4

2 NO AUTHENTICATION

3 DEFAULT TABLESPACE users

4 TEMPORARY TABLESPACE temp

5 QUOTA 100M ON users;

SQL> GRANT

2 CREATE SESSION,

3 CREATE TABLE

4 TO tecatech\_lab2\_4;

SQL> ALTER USER tecatech\_lab2\_4 GRANT CONNECT THROUGH manager;

SQL> COLUMN username FORMAT A32;

SQL> COLUMN account\_status FORMAT A16;

SQL> COLUMN authentication\_type FORMAT A32;

SQL> SELECT

2 username,

3 account\_status,

4 authentication\_type

5 FROM dba\_users

6 WHERE username = 'TECATECH\_LAB2\_4';

SQL> CONNECT tecatech\_lab2\_4/gamma@"DESKTOP-UG7SO1F:1521/xepdb1";

SQL> CONNECT manager[tecatech\_lab2\_4]/default@"DESKTOP-UG7SO1F:1521/xepdb1";

SQL> CREATE TABLE timestamps(

2 timestamp\_id NUMBER(4, 0) NOT NULL,

3 day NUMBER(2, 0),

4 month NUMBER(2, 0),

5 year NUMBER(4, 0),

6 PRIMARY KEY (timestamp\_id)

7 );

SQL> GRANT

2 SELECT,

3 INSERT,

4 UPDATE,

5 DELETE

6 ON timestamps

7 TO tecatech\_lab1\_4;

SQL> CONNECT tecatech\_lab1\_4/alpha@"DESKTOP-UG7SO1F:1521/xepdb1";

SQL> INSERT ALL

2 INTO tecatech\_lab2\_4.timestamps(timestamp\_id, day, month, year) VALUES (1, 10, 6, 2022)

3 INTO tecatech\_lab2\_4.timestamps(timestamp\_id, day, month, year) VALUES (2, 31, 8, 2022)

4 INTO tecatech\_lab2\_4.timestamps(timestamp\_id, day, month, year) VALUES (3, 1, 1, 2023)

5 INTO tecatech\_lab2\_4.timestamps(timestamp\_id, day, month, year) VALUES (4, 31, 1, 2023)

6 INTO tecatech\_lab2\_4.timestamps(timestamp\_id, day, month, year) VALUES (5, 10, 6, 2023)

7 SELECT \* FROM dual;

SQL> SELECT \* FROM tecatech\_lab2\_4.timestamps;

SQL> DROP TABLE tecatech\_lab2\_4.timestamps;

SQL> CONNECT manager[tecatech\_lab2\_4]/default@"DESKTOP-UG7SO1F:1521/xepdb1";

SQL> SELECT \* FROM timestamps;

SQL> CONNECT system/tecatech@"DESKTOP-UG7SO1F:1521/xepdb1";

SQL> ALTER USER tecatech\_lab2\_4 ACCOUNT LOCK;

SQL> CONNECT manager[tecatech\_lab2\_4]/default@"DESKTOP-UG7SO1F:1521/xepdb1";

SQL> CONNECT system/tecatech@"DESKTOP-UG7SO1F:1521/xepdb1";

SQL> DROP USER tecatech\_lab2\_4 CASCADE;

SQL> CREATE USER tecatech\_lab2\_4

2 IDENTIFIED BY gamma

3 DEFAULT TABLESPACE users

4 TEMPORARY TABLESPACE temp

5 QUOTA 100M ON users;

SQL> GRANT

2 CREATE SESSION,

3 CREATE TABLE

4 TO tecatech\_lab2\_4;

SQL> CONNECT tecatech\_lab2\_4/gamma@"DESKTOP-UG7SO1F:1521/xepdb1";

SQL> CREATE TABLE timestamps(

2 timestamp\_id NUMBER(4, 0) NOT NULL,

3 day NUMBER(2, 0),

4 month NUMBER(2, 0),

5 year NUMBER(4, 0),

6 PRIMARY KEY (timestamp\_id)

7 );

SQL> GRANT

2 SELECT,

3 INSERT,

4 UPDATE,

5 DELETE

6 ON timestamps

7 TO tecatech\_lab1\_4;

SQL> CONNECT tecatech\_lab1\_4/alpha@"DESKTOP-UG7SO1F:1521/xepdb1";

SQL> INSERT ALL

2 INTO tecatech\_lab2\_4.timestamps(timestamp\_id, day, month, year) VALUES (1, 10, 6, 2022)

3 INTO tecatech\_lab2\_4.timestamps(timestamp\_id, day, month, year) VALUES (2, 31, 8, 2022)

4 INTO tecatech\_lab2\_4.timestamps(timestamp\_id, day, month, year) VALUES (3, 1, 1, 2023)

5 INTO tecatech\_lab2\_4.timestamps(timestamp\_id, day, month, year) VALUES (4, 31, 1, 2023)

6 INTO tecatech\_lab2\_4.timestamps(timestamp\_id, day, month, year) VALUES (5, 10, 6, 2023)

7 SELECT \* FROM dual;

SQL> SELECT \* FROM tecatech\_lab2\_4.timestamps;

SQL> DROP TABLE tecatech\_lab2\_4.timestamps;

SQL> CONNECT system/tecatech@"DESKTOP-UG7SO1F:1521/xepdb1";

SQL> SELECT

2 username,

3 sysdba,

4 sysoper,

5 sysasm,

6 sysbackup,

7 sysdg,

8 syskm

9 FROM v$pwfile\_users

10 WHERE username = 'TECATECH\_LAB2\_4';

SQL> ALTER USER tecatech\_lab2\_4 NO AUTHENTICATION;

SQL> ALTER USER tecatech\_lab2\_4 GRANT CONNECT THROUGH manager;

SQL> COLUMN username FORMAT A32;

SQL> COLUMN account\_status FORMAT A16;

SQL> COLUMN authentication\_type FORMAT A32;

SQL> SELECT

2 username,

3 account\_status,

4 authentication\_type

5 FROM dba\_users

6 WHERE username = 'TECATECH\_LAB2\_4';

SQL> CONNECT tecatech\_lab2\_4/gamma@"DESKTOP-UG7SO1F:1521/xepdb1";

SQL> CONNECT manager[tecatech\_lab2\_4]/default@"DESKTOP-UG7SO1F:1521/xepdb1";

SQL> SELECT \* FROM timestamps;

SQL> CONNECT system/tecatech@"DESKTOP-UG7SO1F:1521/xepdb1";

SQL> ALTER USER tecatech\_lab2\_4 ACCOUNT LOCK;

SQL> CONNECT manager[tecatech\_lab2\_4]/default@"DESKTOP-UG7SO1F:1521/xepdb1";

SQL> SHOW con\_name;

SQL> SHOW PARAMETER os\_authent\_prefix;

SQL> CREATE USER "OPS$DESKTOP-UG7SO1F\TECATECH\_LAB2\_4" IDENTIFIED EXTERNALLY;

SQL> GRANT CREATE SESSION TO "OPS$DESKTOP-UG7SO1F\TECATECH\_LAB2\_4";

SQL> SHOW USER;

SQL> CREATE VIEW career\_mode AS

2 SELECT

3 players.player\_name AS player,

4 clubs.club\_name AS club,

5 national\_teams.national\_team\_name AS national\_team,

6 players.player\_ovr AS rating,

7 players.player\_age AS age

8 FROM

9 players,

10 clubs,

11 national\_teams

12 WHERE

13 players.club\_id = clubs.club\_id AND

14 players.national\_team\_id = national\_teams.national\_team\_id

15 ORDER BY

16 rating DESC,

17 age ASC;

SQL> SELECT \* FROM career\_mode;

SQL> GRANT CREATE SESSION TO manager;

SQL> CREATE ROLE app\_manager\_role IDENTIFIED BY password;

SQL> GRANT SELECT ON administrator.career\_mode TO app\_manager\_role;

SQL> GRANT app\_manager\_role TO manager;

SQL> CONNECT manager/default@"DESKTOP-UG7SO1F:1521/xepdb1";

SQL> SET ROLE app\_manager\_role IDENTIFIED BY password;

SQL> SELECT \* FROM administrator.career\_mode;

SQL> SELECT \* FROM administrator.national\_teams;

SQL> SELECT \* FROM administrator.leagues;

SQL> SELECT \* FROM administrator.clubs;

SQL> SELECT \* FROM administrator.players;