**Lab 9 – Aarish Salam Memon – A20499744**

**PART – 1**

**(1)**

Graphical user interface, text, application, email

Description automatically generated

**Error stating that user SAM does not exist.**

**(2)**

Graphical user interface, text, application, email

Description automatically generated

**GRANT SUCCEEDED.**

**(3)**

Graphical user interface, text, application, email

Description automatically generated

**Cannot Revoke the Privilege that I have not assigned.**

**(4)**

Graphical user interface, text, application, email

Description automatically generated

**Not enough privileges to create Role.**

**(5)**

Graphical user interface, text, application, email

Description automatically generated

**Insufficient privileges to create a role.**

**PART – 2**

1. Graphical user interface

   Description automatically generated with medium confidence

**Commit done and displayed the table**

**(ii)**

Graphical user interface, text, application, email

Description automatically generated

**Inserted a record and commit completed.**

**(iii)**

Graphical user interface, text, application, email

Description automatically generated

**Save point Created.**

**(iv)**

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application, table

Description automatically generated

**In the above query, it enters a row of record displays the table after adding the record then we rollback to the savepoint that means to remove the inserted row and then we add the row again and display the table after added record.**

**(iv)**

Table

Description automatically generated

**In the above query we have inserted a row and created second save point.**

**(v)**

Graphical user interface, text, application, email

Description automatically generated

**One more row/record inserted.**

**(5a)**

Graphical user interface

Description automatically generated

**We rolled back to the second save point and displayed the table.**

**(5b)**

Graphical user interface, text, application

Description automatically generated

**Rolled back to first save point.**

**PROJECT THREE:**

For each of the following scenarios, suggest what steps the DBA the IT Director should perform:

1. Tammy Smyth, a loyal employee who has worked for DDD Incorporated for ten years, announced her retirement and gave the " usual " two weeks’ notice.

**Answer:** If the employee has completed the two week usual notice, then by the end of that the IT Director and DBA should take her devices and clear all the company related data and cache from that because that would be the usual protocol and revoke her role and privileges from the company’s system.

(b) Jennie Sanders, as soon as she was suspected of employee theft, was immediately terminated. She ran the retail department for Big Blue Mart.

**Answer:** Immediately revoke the rights and roles she had also check for the history and work she has been working on. Lodge a formal complaint to the governmental department.

(c) Marina Pappas, who currently works at the research and development facility as a chemist and formulates new products, has been recruited by another department to development the operations research program for the company. She has accepted the new position.

**Answer:** Smoothly process the handing over process, revoke the roles and cut all the sensitive data she had from the previous department with the help of director of the concerned department. Assign new roles and responsibilities for the new position.

**Question 2. What are the best practices to ensure security on a database using such an IDE as SQL Developer?**

**Answer:**

1. Define Roles Properly.
2. Isolate the server.
3. Keep monitoring the database.
4. Regularly update the database to check there are no anomalies.
5. Apply restricted roles and give limited access to users.
6. Take early actions if there is any threat to the database.
7. Choose a safe network.

**Question 3. Distinguish between a role, a profile, and a privilege. Support your answer (Please use APA for your citations)**

**Answer:**

Roles: Roles are usually created by administrators to group the privileges or other roles, it is to make a package of privileges for a user to complete the actions.

Profile: It’s a default package of privileges assigned to a user for a certain project so they can perform all the required actions.

Privileges: Privilege is a permission for any user for any SQL statement, if they have no role or profile assigned and just a specific privilege is allowed so they can only perform that operation.

Citation: Privileges, roles and profiles. (n.d.). Retrieved December 11, 2021, from [Cuddletech](http://cuddletech.com/articles/oracle/node36.html)

**Question 4. What is the danger to assigning / granting to PUBLIC?**

**Answer:** It is a risky scene to assign any role or privilege to public as there might be chances of data theft, and data duplication. There might be a chance that the public user is not a advance level database user and hurts the schema of the database. That is the reason for best practices always define the roles you are assigning to users because in that way there would be a very less chance of corruption and there would be no threat to security. While we can revoke the role assigned to public but still there is no recommendation of going with that in first place.

**Question 5. Charles was given the order to grant specific privileges to Nick on Charles’ table named food\_club\_members. Nick is a new - hire and will be working with Charles to maintain and manipulate important database files for the Eats - a - Lot Corporation.**

**Instead of using the following code for Nick**

**grant All on food\_club\_members to nick\_01\_user;**

**Charles used the code**

**grant All on food\_club\_members to public;**

**which he immediately executed. Some unscrupulous employee began to download the entire food\_club\_members to their flash drive.**

**What actions should the DBA and Charles’ supervisor perform?**

**Answer:**

DBA and the supervisor should immediately revoke all the rights assigned to public. There is no way to revoke the files downloaded in the flash drive but for the further investigation they should track the IP address of the user and match it with the devices in the offices and track down the employee who has downloaded the files.