Task 1. Figure out what security precautions are already used in your 'dvd\_rental' database. Prepare description

To analyze the existing security precautions in the dvd\_rental PostgreSQL database, I executed the following SQL query:

***SELECT rolname, rolsuper, rolcreaterole, rolecreatedb, rolcanlogin***

***FROM pg\_roles;***

This query retrieves a list of all defined roles (users and groups) in the PostgreSQL instance, along with their associated privileges. Specifically:

* rolname: displays the name of the role.
* rolsuper: indicates whether the role has superuser privileges.
* rolcreaterole: shows whether the role can create new roles.
* rolcreatedb: shows whether the role can create new databases.
* rolcanlogin: determines whether the role can log in.

This query provides essential insight into the current security configuration of the database:

* It helps identify which roles have elevated privileges such as ***SUPERUSER***, ***CREATEROLE***, or ***CREATEDB***.
* It clarifies which roles are allowed to ***log in*** and interact directly with the database.
* It also helps distinguish ***between login roles*** (individual users) ***and group roles*** (used for managing permissions collectively).

By reviewing this output, we can evaluate whether the principle of least privilege is being followed, and whether any users have unnecessary or excessive rights that could pose a security risk.

This query returned this information:

Slika na kojoj se nalazi tekst, snimak ekrana, broj, softver

Sadržaj koji generiše veštačka inteligencija može biti netačan.

This shows that only the default postgres role has superuser privileges, can create roles and databases, and is allowed to log in. All other predefined PostgreSQL system roles (like pg\_monitor, pg\_read\_all\_data, etc.) do not have login permissions and are not superusers — they exist solely to be granted specific capabilities to users as needed.

This confirms that the current security configuration follows the principle of least privilege: only necessary access is granted, and no extra roles with high privileges are present.