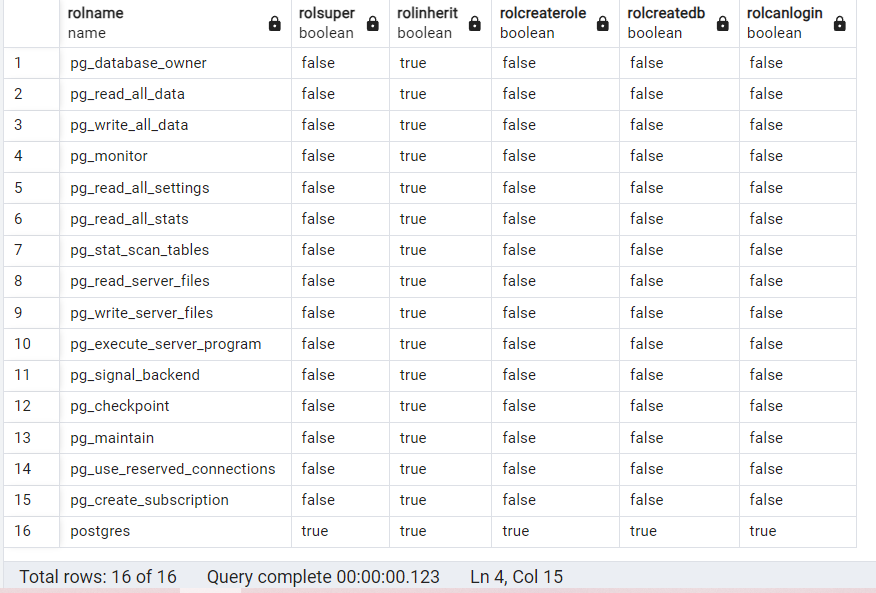
**Task 1.** Figure out what security precautions are already used in your 'dvd\_rental' database. Prepare description

1. Check User Roles and Privileges

-- Check role-specific privileges

SELECT rolname, rolsuper, rolinherit, rolcreaterole, rolcreatedb, rolcanlogin

FROM pg\_roles;

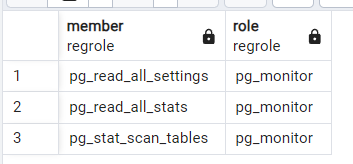


1. Check Role Memberships

-- Show role memberships

SELECT roleid::regrole AS member, member::regrole AS role

FROM pg\_auth\_members;

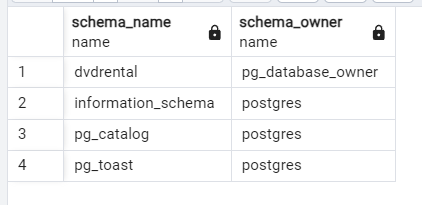


1. Check Database Object Permissions

-- List all schemas and their owners

SELECT schema\_name, schema\_owner

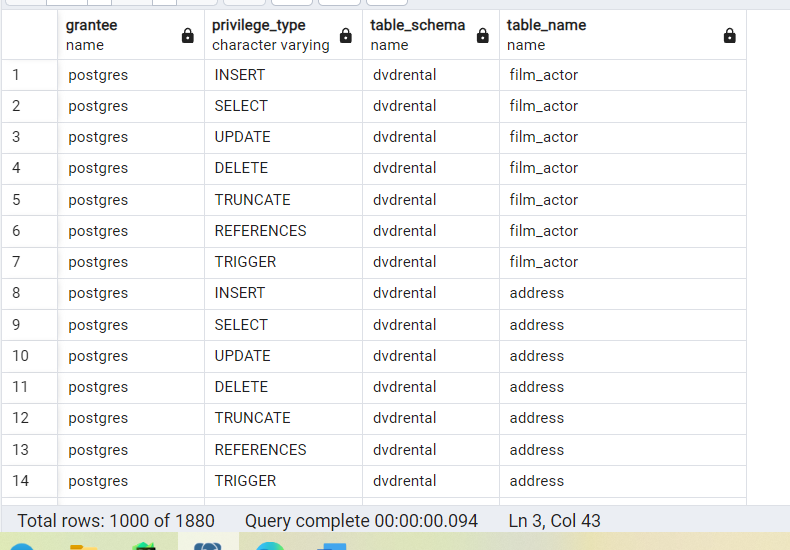
FROM information\_schema.schemata;



-- Check table privileges

SELECT grantee, privilege\_type, table\_schema, table\_name

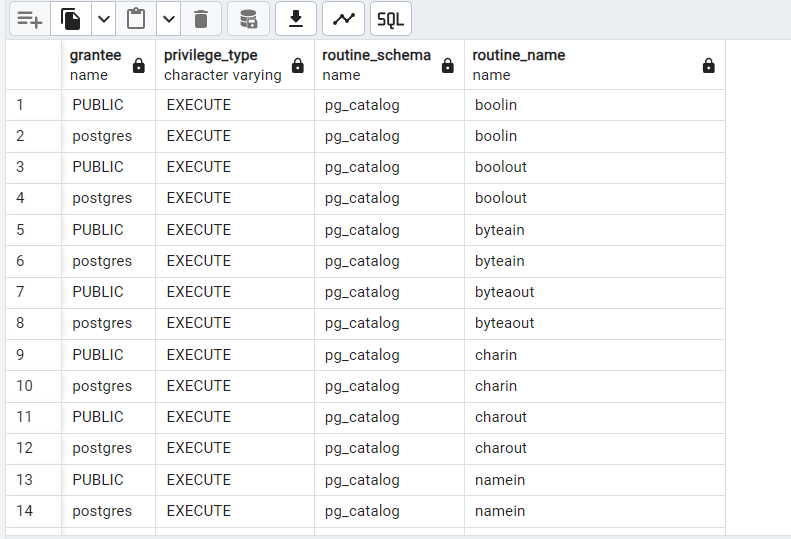
FROM information\_schema.role\_table\_grants;



-- Check function privileges

SELECT grantee, privilege\_type, routine\_schema, routine\_name

FROM information\_schema.role\_routine\_grants;



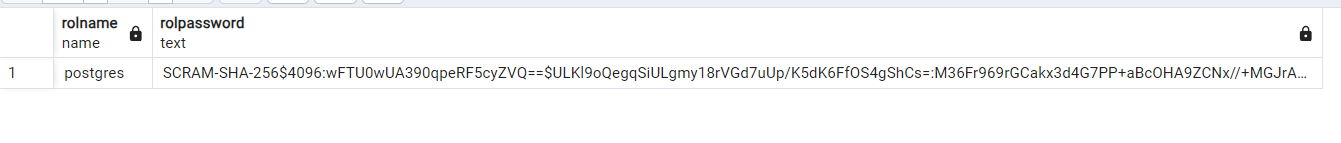
1. Password and Authentication

-- Check password-encryption status

SELECT rolname, rolpassword

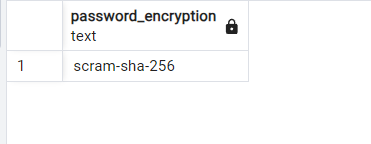
FROM pg\_authid

WHERE rolpassword IS NOT NULL;



-- Check the PostgreSQL configuration for authentication

SHOW password\_encryption;



1. Database-Level Security Settings

-- Check security-related settings

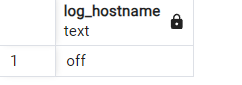
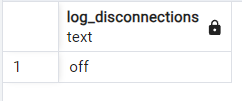
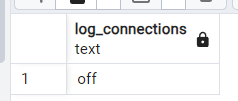
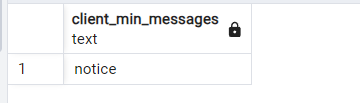
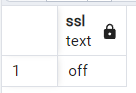
SHOW ssl; -- SSL enabled

SHOW client\_min\_messages; -- Minimum log level for client connections

SHOW log\_connections; -- Logging connection attempts

SHOW log\_disconnections; -- Logging disconnections

SHOW log\_hostname; -- Logging client hostname



1. Monitor and Detect Intrusions

-- Look for extensions or audit tools

SELECT extname, extversion

FROM pg\_extension;

