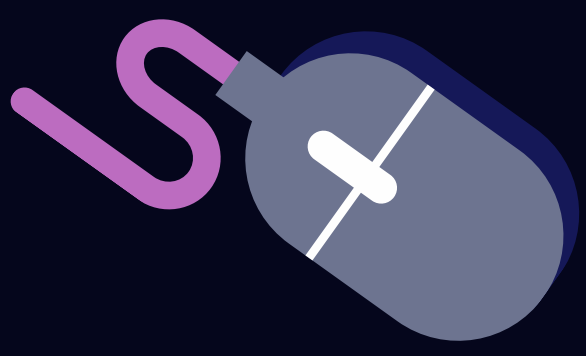
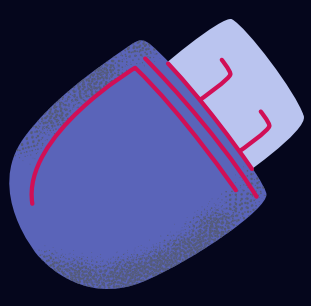
RLS BYPASS

Bypassing Row-Level Security (RLS) in PostgreSQL refers to mechanisms that allow specific users, roles, or operations to ignore RLS policies and access restricted data. RLS enforces to access control at the row level, but scenarios like administrative tasks, system-level functions, or performance optimization may require bypassing these restrictions.

why RLS is needed?

- Protect sensitive data.
- Compliance.
- Multi-tenant apps.
- Minimize insider threats.





Core Methods

- BYPASSRLS Role Attribute
- Security-Definer Functions/ Views
- Direct Table Access

Perfomance & security risks

- RLS policies add query overhead. Bypassing can speed up bulk operations but risks exposing sensitive data.
- Data breaches

Best Practices

- Least Privilege: Grant BYPASSRLS only to admins.
- Test Policies: Use EXPLAIN to verify filters.
- Avoid SECURITY DEFINER: Default to SECURITY INVOKER.
- Encrypt Sensitive Data: Layer RLS with encryption.

Summary

- RLS is critical but not foolproof.
- Combine with least privilege, testing, and layered security.
- Regularly audit policies and permissions.