Permissions granted:

- CONNECT – applicant_data database; allows app_user to open connection to the database
- USAGE – public schema; required to reference any table or sequence in the schema
- SELECT – applicants table; run_queries() runs 14 analysis queries; fix_uc_universities() reads rows to re-normalize
- INSERT – applicants table; insert_row() adds newly scraped entries from GradCafe
- UPDATE – applicants table; fix_gre_aw() nullifies invalid scores; fix_uc_universities() corrects campus names
- USAGE, SELECT – applicants_p_id_seg sequence; the p_id SERIAL PRIMARY KEY column auto-increments on each INSERT which requires advancing the sequence

Not granted:

- DELETE – the app never deletes rows
- TRUNCATE – the app never truncates tables
- DROP – the app never drops tables at runtime
- ALTER – the app never modifies schema
- CREATE – the app never creates tables at runtime (load_data.py does, but that runs as a superuser during initial setup)

SQL snippet:

```
-- Least-privilege database user for the applicant_data application.
--
-- Run this script as a superuser (e.g., postgres) AFTER load_data.py
-- has created the database and table:
--
--   psql -U postgres -d applicant_data -f src/create_app_user.sql
--
-- Then configure the app to connect as app_user via environment variables:
--
--   export
DATABASE_URL="postgresql://app_user:change_me@localhost:5432/applicant_data"

-- 1. Create the application user
DO $$
BEGIN
    IF NOT EXISTS (SELECT 1 FROM pg_roles WHERE rolname = 'app_user') THEN
        CREATE USER app_user WITH PASSWORD 'change_me';
    END IF;
END
$$;
```

```sql
-- 2. Allow connecting to the database
GRANT CONNECT ON DATABASE applicant_data TO app_user;

-- 3. Allow usage of the public schema
GRANT USAGE ON SCHEMA public TO app_user;

-- 4. Grant only the permissions the app needs on the applicants table:
--    SELECT  — query_data.run_queries(), cleanup_data.fix_uc_universities()
--    INSERT  — app.insert_row()
--    UPDATE  — cleanup_data.fix_gre_aw(), cleanup_data.fix_uc_universities()
GRANT SELECT, INSERT, UPDATE ON TABLE applicants TO app_user;

-- 5. Allow the SERIAL primary key to auto-increment on INSERT
GRANT USAGE, SELECT ON SEQUENCE applicants_p_id_seq TO app_user;

-- Permissions NOT granted (least privilege):
--   DELETE   — the app never deletes rows
--   TRUNCATE — the app never truncates tables
--   DROP     — the app never drops tables
--   ALTER    — the app never alters schema
--   CREATE   — the app never creates tables at runtime
```