

### Step 3:

```
[postgres=# CREATE USER app_least_priv_user; Our app must read DB connection values from environment variables, for example:  
ERROR:  role "app_least_priv_user" already exists  
[postgres=# GRANT CONNECT ON DATABASE postgres TO app_least_priv_user;  
GRANT  
[postgres=# GRANT USAGE ON SCHEMA public TO app_least_priv_user; DB_HOST , DB_NAME , DB_USER , DB_PASSWORD  
GRANT  
[postgres=# GRANT SELECT, INSERT ON TABLE applicants TO app_least_priv_user;  
GRANT  
[postgres=# GRANT USAGE, SELECT ON SEQUENCE applicants_p_id_seq TO app_least_priv_user;  
GRANT  
[postgres=# ] Do not commit real secrets. Ensure .env is in .gitignore..
```

GRANT CONNECT... allows the user to connect to the database

GRANT USAGE ON SCHEMA... allows the user to access objects stored in the public schema ( where 'applicants' table is located)

GRANT SELECT/INSERT.... SELECT allows the reader to read existing data points in the table and INSERT allows the user to add new datapoints to the table(Flask needs to pull data to be displayed and add new data points when scrape.py is iterated)

GRANT USAGE/SELECT... SEQUENCE... grants permission to interact with the autogenerated p\_id primary key (needed to prevent permission errors when adding new data if p\_id is untouchable)

The screenshot shows a PostgreSQL roles management interface. On the left, there's a sidebar with links for Home, Modules, Assignments, Grades, and People. A notification bubble indicates 9 pending changes. The main area is titled 'Privileges Required' and lists two roles:

Role name	Attributes	Member of
app_least_priv_user	Superuser, Create role, Create DB, Replication, Bypass RLS	
harryma		

A note above the roles states: "Security is not just query syntax. Your database account should have the minimum privileges needed."

The right side of the screen has a section titled "Required changes" with the following steps:

1. No hard-coded DB credentials in code.  
Your app must read DB connection values from environment variables, for example:
  - DB\_HOST , DB\_PORT , DB\_NAME , DB\_USER , DB\_PASSWORD
2. Include a file named `.env.example` containing the variable names (with placeholder values).  
Do not commit real secrets. Ensure `.env` is in `.gitignore`.

### Step 4:

Three main dependencies feed into the core application: python-dotenv, Flask, and psycopg. Dotenv acts as the foundational layer for security, loading sensitive credentials from environment variables to ensure the DATABASE\_URL is never hard-coded, which is a key requirement for portable CI/CD environments. Flask serves as the primary web framework, utilizing Blueprints for modular routing and Jinja2 templating to render the analysis page with the required "Answer:" labels and two-decimal formatting. Within the Flask ecosystem, the jsonify utility is critical for implementing "busy-state" behavior, allowing the API to return specific 409 Conflict status codes when a data pull is already in progress. To manage the data layer, psycopg2 provides the necessary adapter for PostgreSQL communication, using connection objects and cursors to execute the idempotent INSERT queries that prevent duplicate records. Together, these dependencies enable a testable architecture where the database logic, web routing, and environment configuration remain decoupled and secure.

#### Step 5:

Adding a setup.py file to the project directory is a critical step for ensuring long-term maintainability and professional distribution. This configuration file effectively transforms a collection of individual scripts into a formal Python package, allowing for a standardized installation process across various environments. By defining the project structure this way, developers can ensure that internal module imports remain consistent whether the code is executing on a local workstation, within a testing suite, or throughout a continuous integration pipeline. Furthermore, the inclusion of a setup.py facilitates editable installs, which allows the environment to reflect code changes in real time while maintaining correct system paths. This practice also enables modern dependency managers like uv to accurately synchronize the environment, providing a robust foundation for reproducible research and development.

#### Step 6:

Initial run:

```
Successfully installed flask 2.1.5 werkzeug 2.1.0
(.venv) harryma@Harrys-MacBook-Pro-2 module_5 % snyk test

Testing /Users/harryma/Modern Software Concepts/jhu_software_concepts/module_5...
Tested 66 dependencies for known issues, found 1 issue, 1 vulnerable path.

Issues with no direct upgrade or patch:
  ✘ Deserialization of Untrusted Data [High Severity] [https://security.snyk.io/vuln/SNYK-PYTHON-DISKCACHE-15268422] in diskcache@5.6.3
    introduced by llama-cpp-python@0.2.90 > diskcache@5.6.3
    No upgrade or patch available
```

Organization: harryma-jhu

Fixed: (.snyk file created)

```
(.venv) harryma@Harrys-MacBook-Pro-2 module_5 % snyk test

Testing /Users/harryma/Modern Software Concepts/jhu_software_concepts/module_5...
Organization: harryma-jhu
Package manager: pip
Target file: requirements.txt
Project name: module_5
Open source: no
Project path: /Users/harryma/Modern Software Concepts/jhu_software_concepts/module_5
Local Snyk policy: found
Licenses: enabled

✓ Tested 66 dependencies for known issues, no vulnerable paths found.
```

Extra credit (Snyk Code):

```
Testing /Users/harryma/Modern Software Concepts/jhu_software_concepts/module_5 ...
```

#### Open Issues

```
x [MEDIUM] Debug Mode Enabled
  Finding ID: ba1b00e6-dbb4-47da-b958-544eefab45db
  Path: src/app.py, line 100
  Info: Running the application in debug mode (debug flag is set to True in run) is a
        security risk if the application is accessible by untrusted parties.
```

#### Test Summary

```
Organization:      harryma-jhu
Test type:        Static code analysis
Project path:     /Users/harryma/Modern Software Concepts/jhu_software_concepts/mo
dule_5
Total issues:    1
Ignored issues:  0 [ 0 HIGH  0 MEDIUM  0 LOW ]
Open issues:     1 [ 0 HIGH  1 MEDIUM  0 LOW ]
```

#### Tip

To view ignored issues, use the `--include-ignores` option.

```
(.venv) harryma@Harrys-MacBook-Pro-2 module_5 %
```

This makes sense since debug is still set to True in app.py to help with instant feedback on the webpage with changes I've made in the code. Eventually, this will be turned to False and the 1 open issue will be resolved.