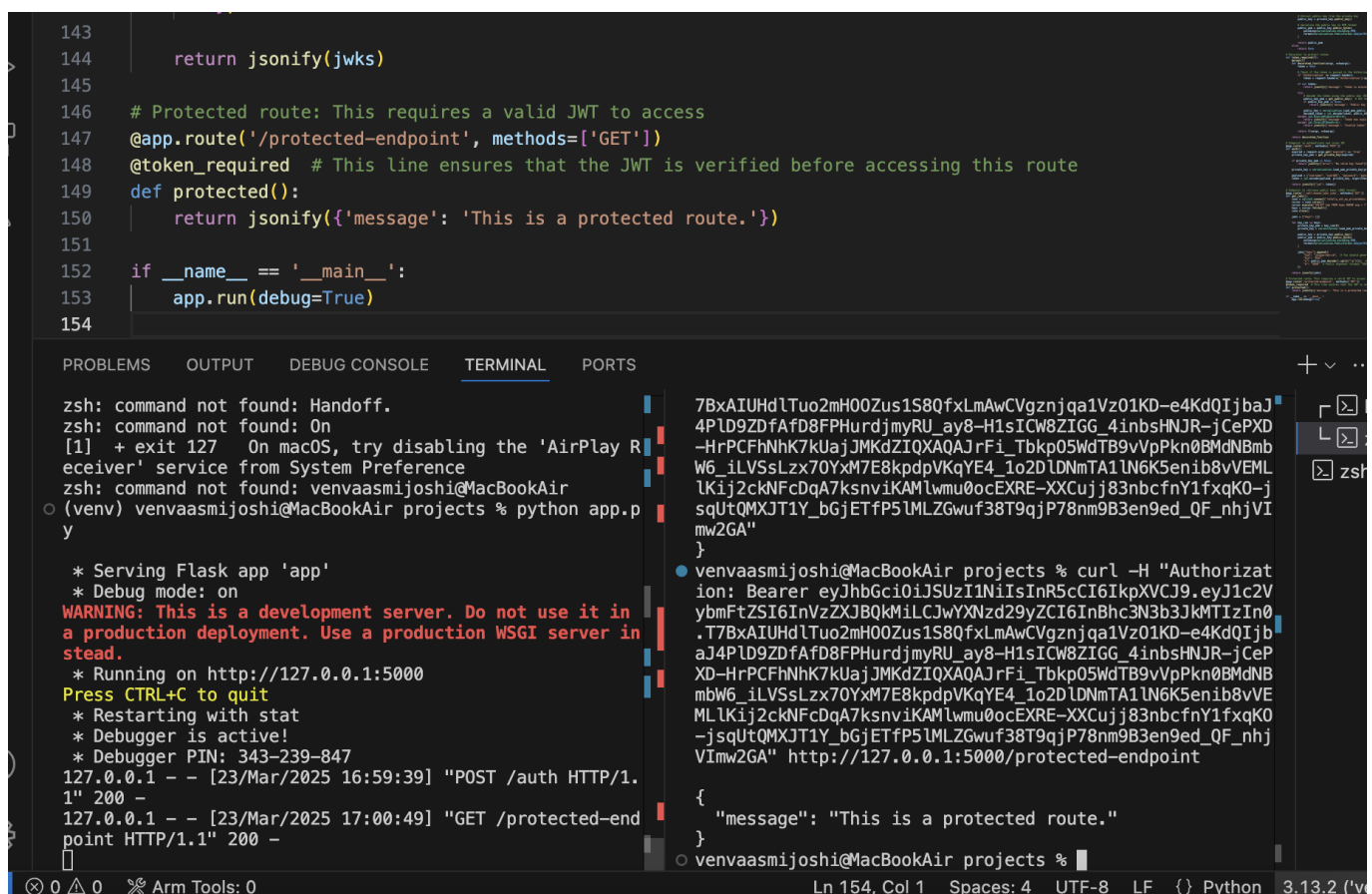# README for Project 2

Introduction:

This project involves extending the basic JWKS (JSON Web Key Set) server with SQLite-backed

storage for private keys. The goal is to store private keys securely and provide functionality for

signing JWTs and verifying them using the JWKS endpoint. Additionally, SQL injection prevention is

a focus when interacting with the SQLite database.

Top screenshot

Left terminal:

```
zsh: command not found: Handoff.
zsh: command not found: On
[1]  + exit 127   On macOS, try disabling the 'AirPlay R
eceiver' service from System Preference
zsh: command not found: venvaasmijoshi@MacBookAir
(venv) venvaasmijoshi@MacBookAir projects % python app.p
y

 * Serving Flask app 'app'
 * Debug mode: on
WARNING: This is a development server. Do not use it in
a production deployment. Use a production WSGI server in
stead.
 * Running on http://127.0.0.1:5000
Press CTRL+C to quit
 * Restarting with stat
 * Debugger is active!
 * Debugger PIN: 343-239-847
127.0.0.1 - - [23/Mar/2025 16:59:39] "POST /auth HTTP/1.
1" 200 -
127.0.0.1 - - [23/Mar/2025 17:00:49] "GET /protected-end
point HTTP/1.1" 200 -
```

Right terminal:

```
venvaasmijoshi@MacBookAir projects % curl -X POST http:/
/127.0.0.1:5000/auth
```

{
  "jwt": "eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2Vyb
mFtZSI6InVzZXJBQkMiLCJwYXNzd29yZCI6InBhc3N3b3JkMTIzIn0.T
7BxAIUHdlTuo2mHOOZus1S8QfxLmAwCVgznjqa1Vz01KD-e4KdQIjbaJ
4PlD9ZDfAfD8FPHurdjmyRU_ay8-H1sICW8ZIGG_4inbsHNJR-jCePXD
-HrPCFhNhK7kUajJMKdZIQXAQAJrFi_Tbkp05WdTB9vVpPkn0BMdNBmb
W6_iLVSsLzx70YxM7E8kpdpVKqYE4_1o2DlDNmTA1lN6K5enib8vVEML
lKij2ckNFcDqA7ksnviKAMlwmu0ocEXRE-XXCujj83nbcfnY1fxqKO-j
sqUtQMXJT1Y_bGjETfP5lMLZGwuf38T9qjP78nm9B3en9ed_QF_nhjVI
mw2GA"
}

```
venvaasmijoshi@MacBookAir projects % curl -H "Authorizat
ion: Bearer eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2V
ybmFtZSI6InVzZXJBQkMiLCJwYXNzd29yZCI6InBhc3N3b3JkMTIzIn0
.T7BxAIUHdlTuo2mHOOZus1S8QfxLmAwCVgznjqa1Vz01KD-e4KdQIjb
aJ4PlD9ZDfAfD8FPHurdjmyRU_ay8-H1sICW8ZIGG_4inbsHNJR-jCeP
XD-HrPCFhNhK7kUajJMKdZIQXAQAJrFi_Tbkp05WdTB9vVpPkn0BMdND
mbW6_iLVSsLzx70YxM7E8kpdpVKqYE4_1o2DlDNmTA1lN6K5enib8vVE
MLlKij2ckNFcDqA7ksnviKAMlwmu0ocEXRE-XXCujj83nbcfnY1fxqKO
-jsqUtQMXJT1Y_bGjETfP5lMLZGwuf38T9qjP78nm9B3en9ed_QF_nhj
```

Bottom screenshot

Left terminal:

```
 * Serving Flask app 'app'
 * Debug mode: on
WARNING: This is a development server. Do no
t use it in a production deployment. Use a p
roduction WSGI server instead.
 * Running on http://127.0.0.1:5000
Press CTRL+C to quit
 * Restarting with stat
 * Debugger is active!
 * Debugger PIN: 343-239-847
127.0.0.1 - - [23/Mar/2025 16:59:39] "POST /
auth HTTP/1.1" 200 -
127.0.0.1 - - [23/Mar/2025 17:00:49] "GET /p
rotected-endpoint HTTP/1.1" 200 -
 * Detected change in '/Users/aasmijoshi/pro
jects/test_app.py', reloading
 * Restarting with stat
 * Debugger is active!
 * Debugger PIN: 343-239-847
^C
(venv) venvaasmijoshi@MacBookAir projects %
```

Right terminal:

```
Using cached packaging-24.2-py3-none-any.whl
 (65 kB)
Installing collected packages: pluggy, packa
ging, iniconfig, pytest
Successfully installed iniconfig-2.1.0 packa
ging-24.2 pluggy-1.5.0 pytest-8.3.5

[notice] A new release of pip is available:
25.0 -> 25.0.1
[notice] To update, run: pip install --upgra
de pip
venvaasmijoshi@MacBookAir projects % pytest

=========== test session starts ============
platform darwin -- Python 3.13.2, pytest-8.3
.5, pluggy-1.5.0
rootdir: /Users/aasmijoshi/projects
collected 2 items

test_app.py ..                      [100%]

============ 2 passed in 0.26s =============
```