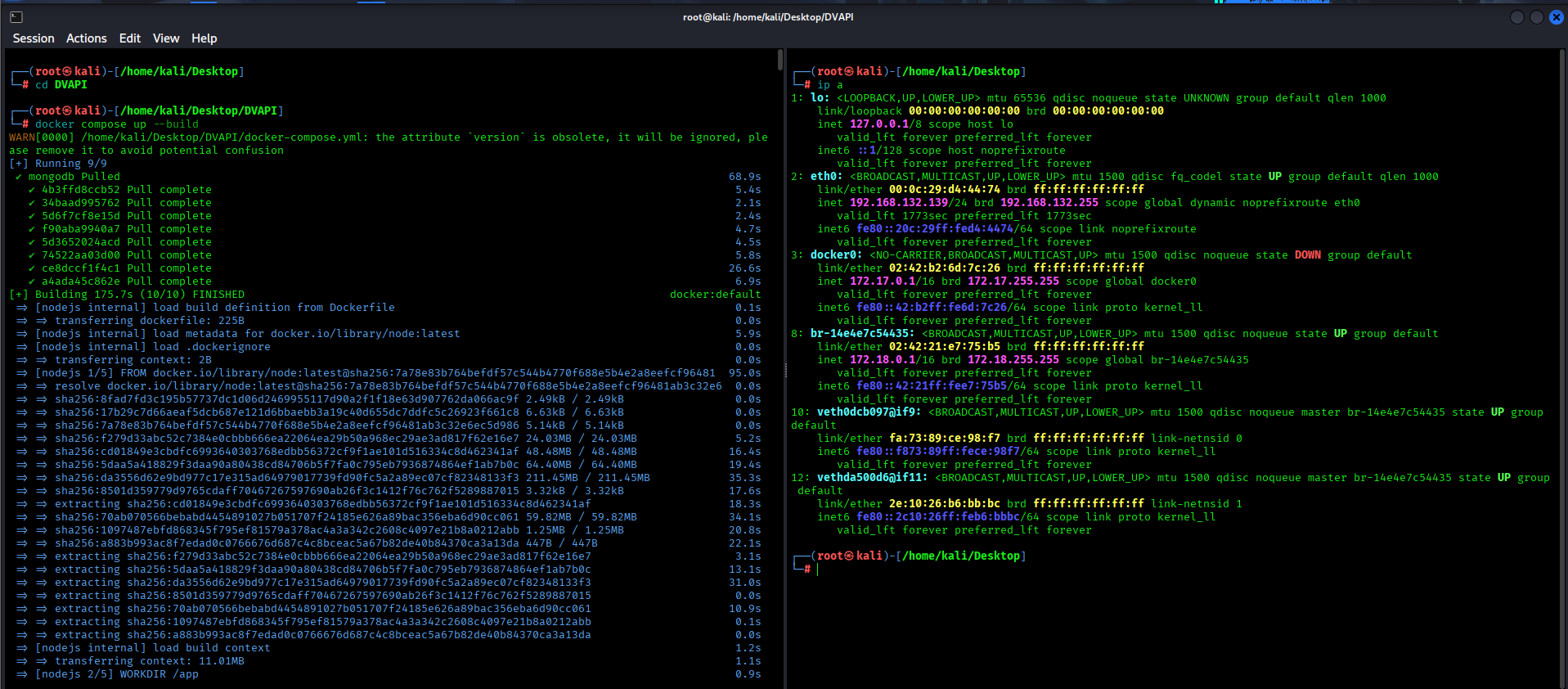
## ****Lab 2 — API Security Checklist (DVAPI)****

**Target:** http://127.0.0.1:3000 (DVAPI local)  
**Tools Used:** Docker, Browser, Postman, Kali Linux (optional)  
**Author:** Ishan Chowdhury

### ****Checklist****

**Setup / Start DVAPI**

Pull and run DVAPI container (replace image name you used)



**Account creation & login**

Register a new user in the DVAPI UI.

Login via browser and confirm dashboard/ui access

**Capture auth token from browser**

Open DevTools → Network → filter XHR.

Perform a login or an authenticated request; copy Authorization: Bearer token from the request headers.

**Configure Postman**

New request → add header:

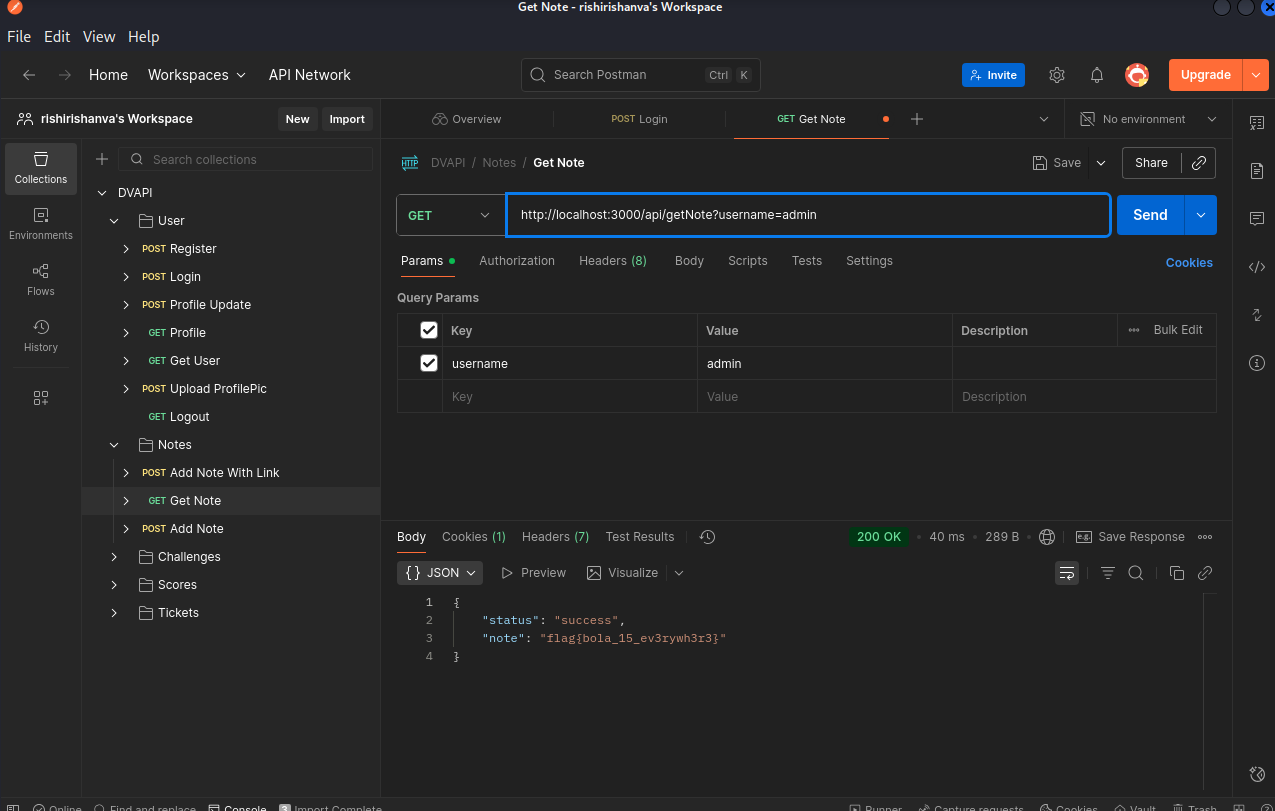
Authorization: Bearer token

Content-Type: application/json (or appropriate)

Save collection as DVAPI-Lab.

**BOLA — enumerate /api/users and retrieve flag by changing user param**

Identify user/notes endpoint, example: GET http://127.0.0.1:3000/api/notes



**Insecure file upload — profile picture abuse to obtain flag**

Find upload endpoint (example): POST http://127.0.0.1:3000/api/profile/upload (or as in DVAPI)

In Postman: choose Body → form-data, add file field (e.g. file), and select an image > 60 MB.

Or use curl (adjust endpoint & field name):

curl -X POST "http://127.0.0.1:3000/api/profile/upload" \

-H "Authorization: Bearer <TOKEN>" \

-F ["file=@/path/to/large-image-61MB.jpg"](mailto:\"file=@/path/to/large-image-61MB.jpg\")

