To start the database:

sudo docker compose -f 'docker-compose.yml' up -d --build

How to achieve the web server now:

go build -o ./bin/main ./cmd/ && sudo setcap 'cap_net_bind_service=+ep' ./bin/main && ./bin/main

To setup the environment:

sudo apt update
sudo apt install snapd -y

sudo apt install git -y

sudo snap install go --classic

sudo snap install code --classic

sudo snap install zaproxy --classic

sudo snap install docker

sudo apt install graphviz -y

go install github.com/google/pprof@latest

To stop the web server:

Ctrl + c

Set up the web server:

You must manually register with the account name: tempuser, other part is not that matter, but consider the password and recover are: comp4334password / comp4334recover

You must try login with the account, if the login page show error: Fail to generate the token

Stop the web server

Go to the :

📦 cmd
 ┣ 📂 api
.....
 ┗ 📜 main.go <--

Manually set the drop_flag to true

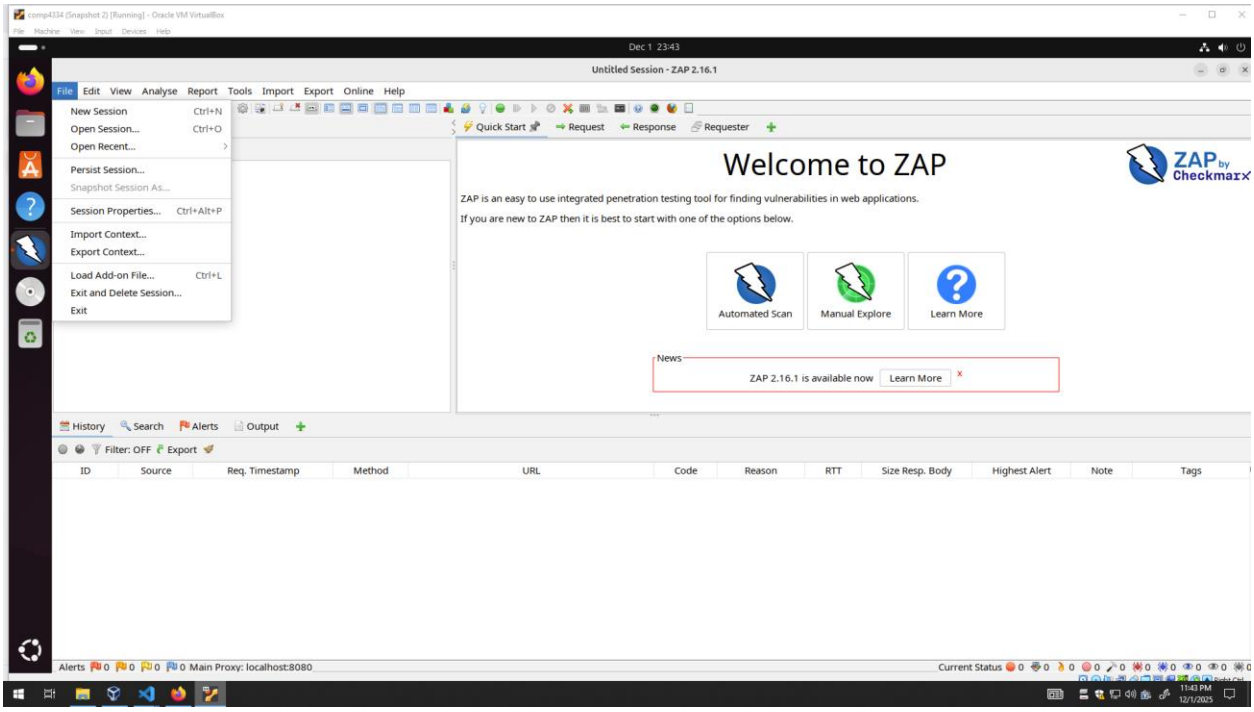
Restart the web server, due to the database do not having the key that insert into database.

Such that drop the database and restart the initialization database process.

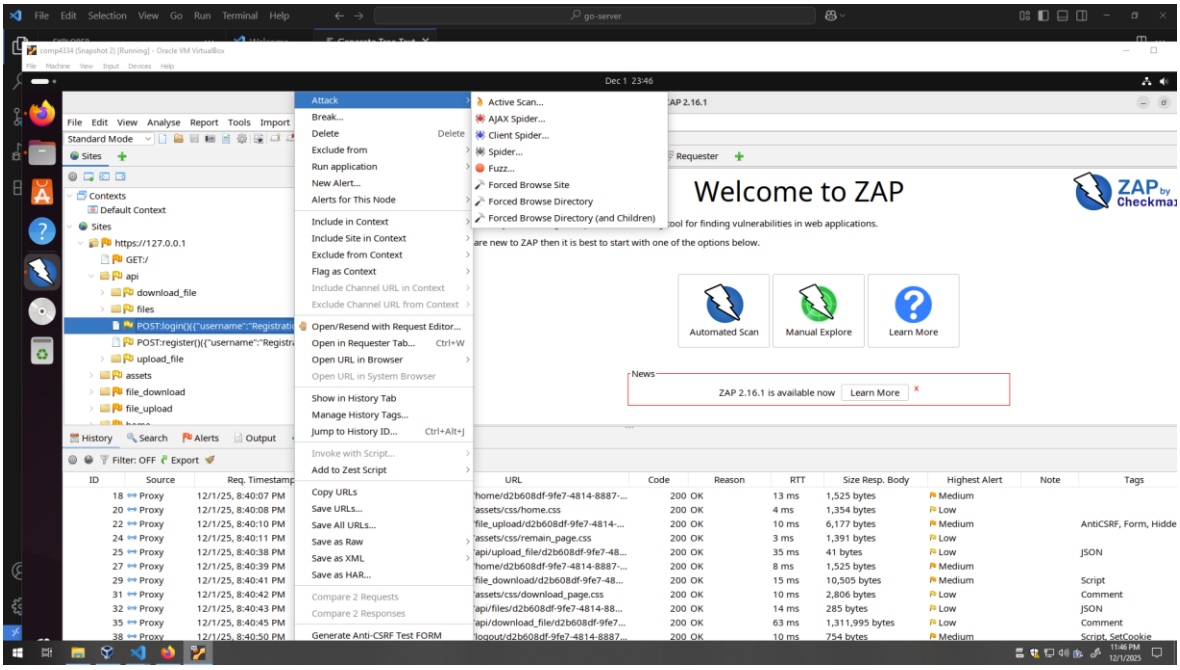
Open the zap:

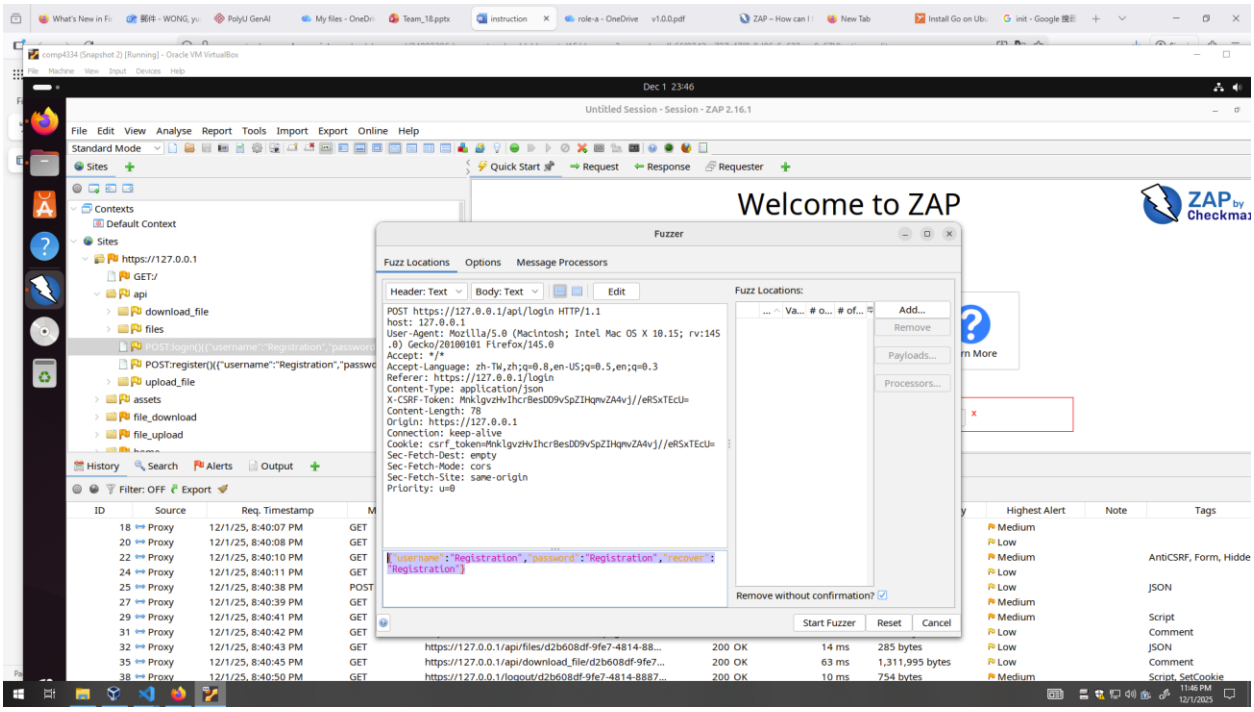
Import the session:

File -> open the session , choose the session

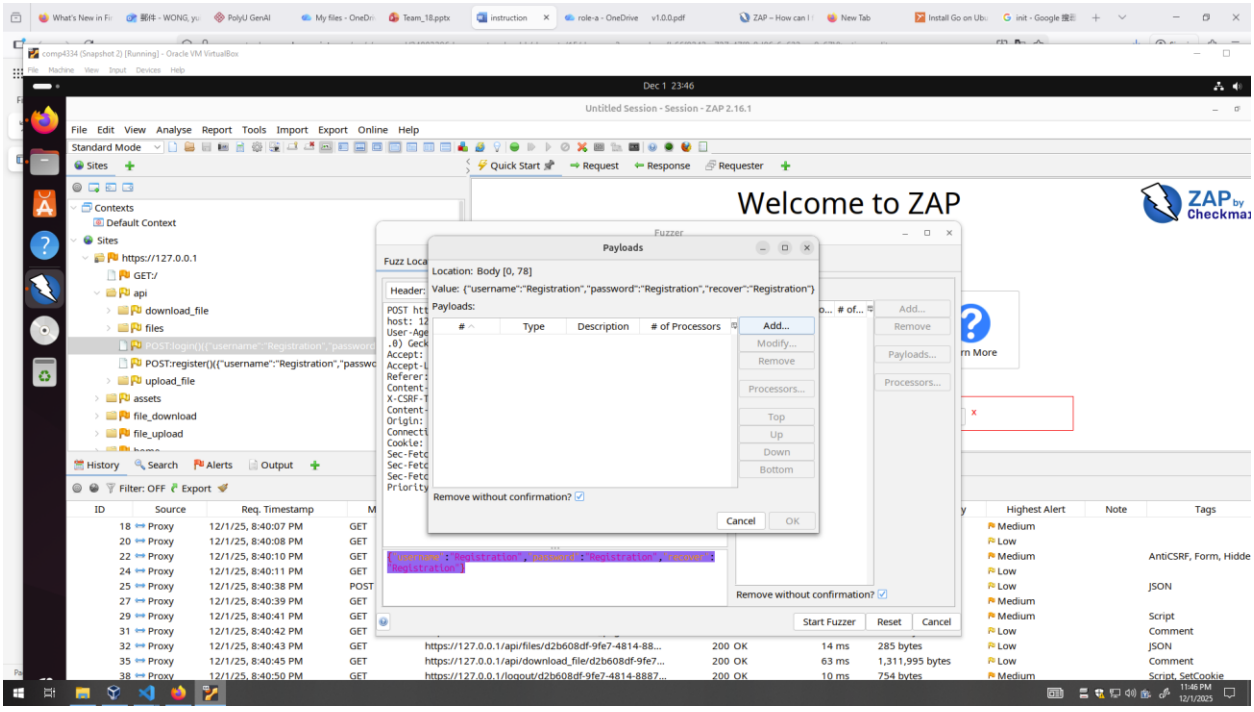


Choose the fuzz:

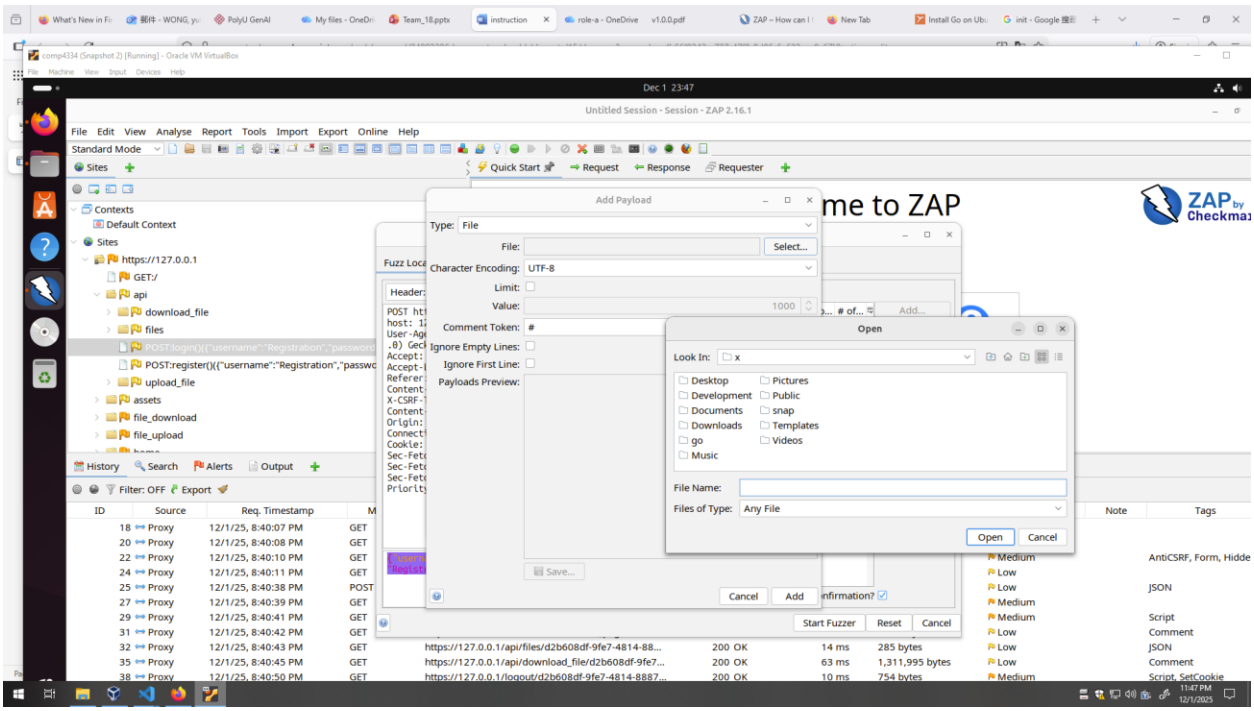




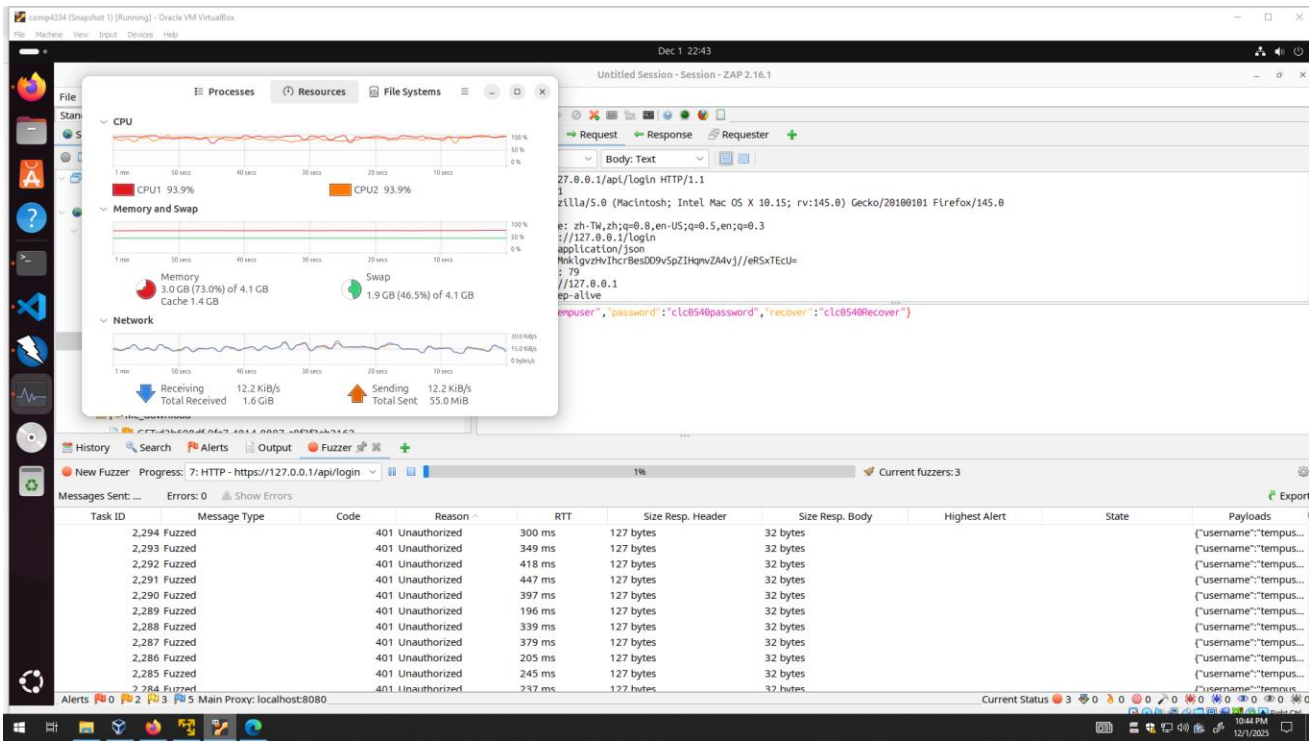
, add

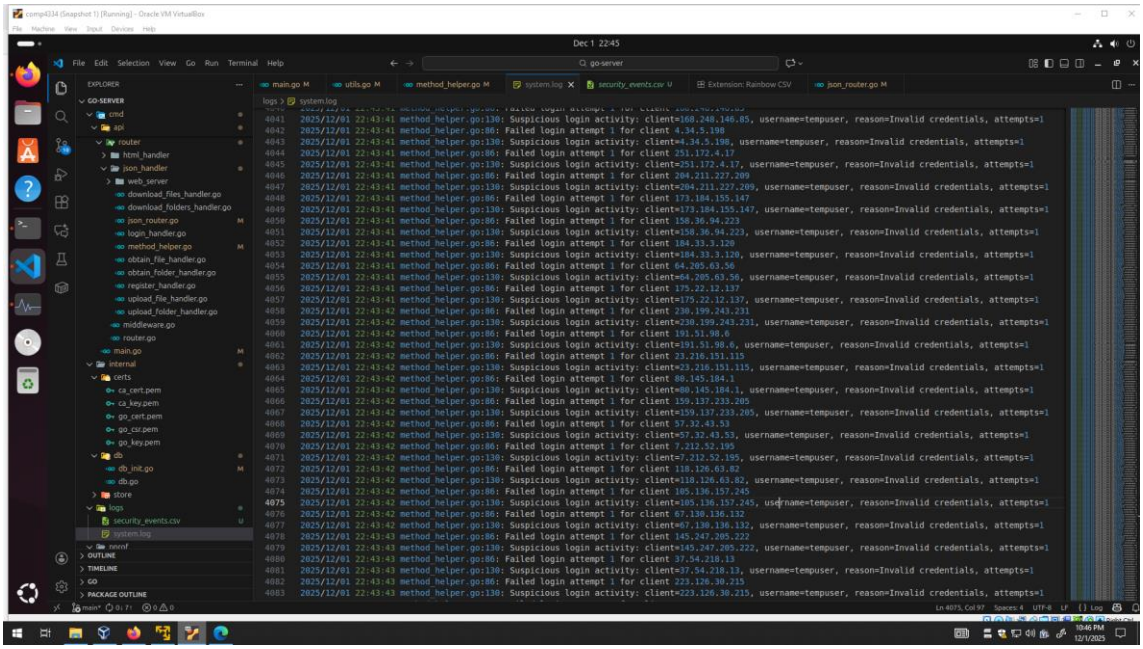


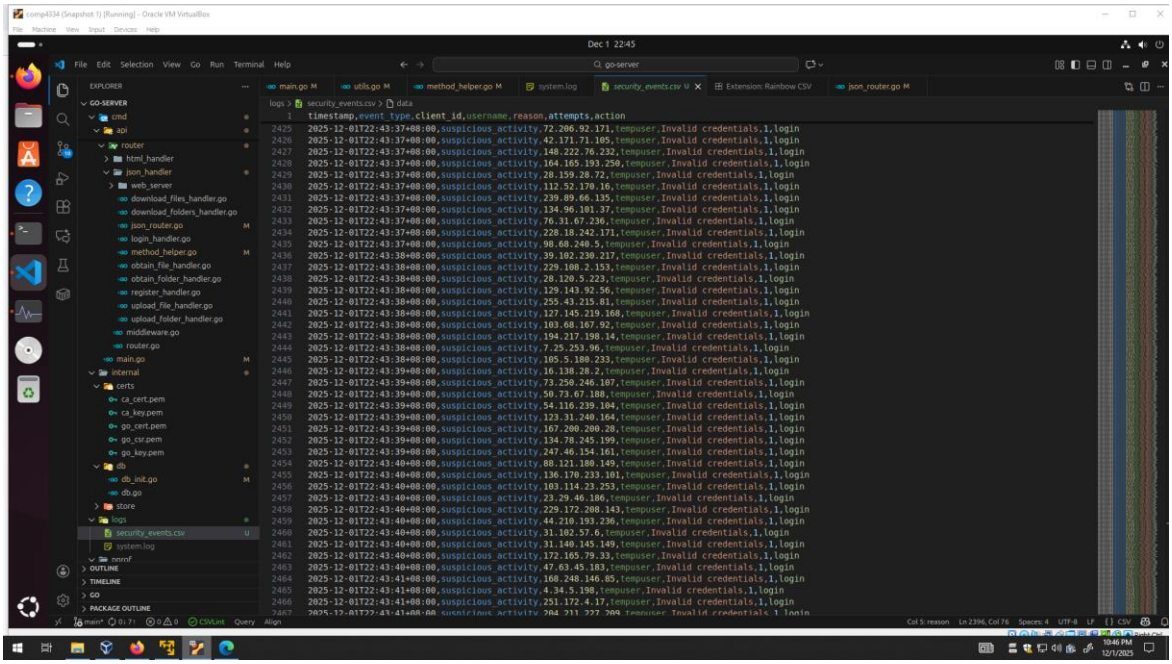
, import the txt payload file



, start the fuzzer, Result







analyze the data:

sudo apt install graphviz -y

go install github.com/google/pprof@latest

go tool pprof -http=:6060 cpu/heap_*.pprof