Lab 4 – LLM Agent Deployment Report

This report documents the setup, deployment, and validation of a Large Language Model (LLM) Agent environment using Docker and the Agent Framework DevUI. The objective of this lab was to build a working agent-based system, configure secure API access, and validate its operation.

Environment Setup

We configured a Docker-based environment using docker-compose. The system includes a DevUI service running on port 8080 and connected to the Groq OpenAI-compatible API endpoint. The agent framework runs inside a container built from a custom Dockerfile and managed via Docker Compose.

API Configuration

An API key was securely injected into the container using environment variables defined in the .env file. This ensured safe authentication without hardcoding sensitive credentials in the source code. The LLM backend is powered by GROQ for fast inference.

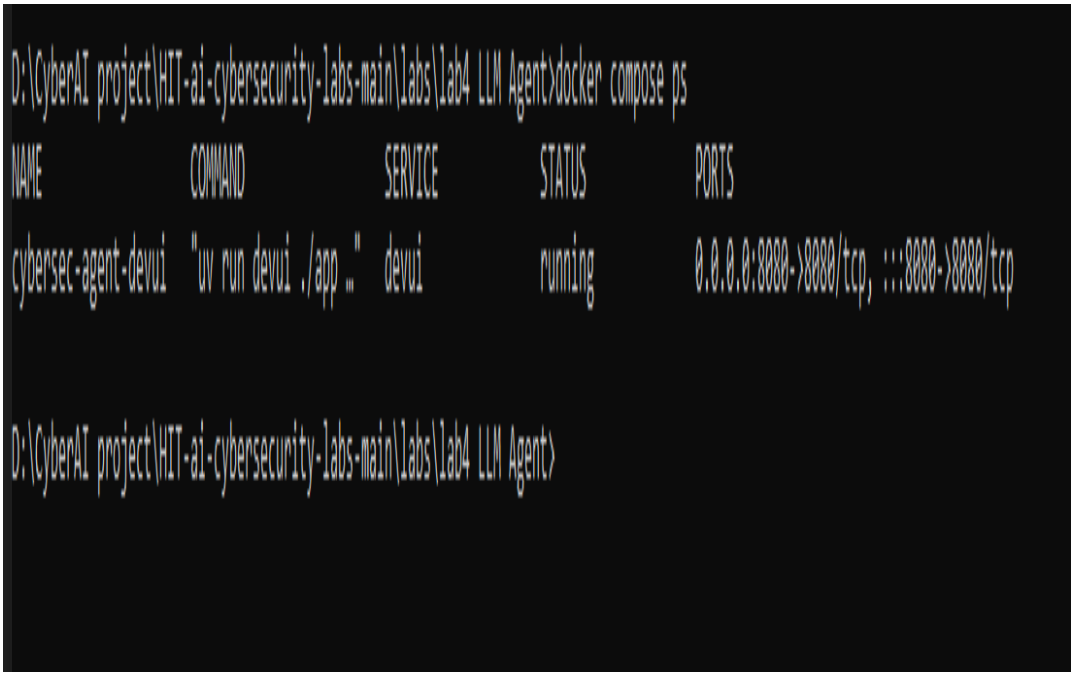
Deployment & Validation

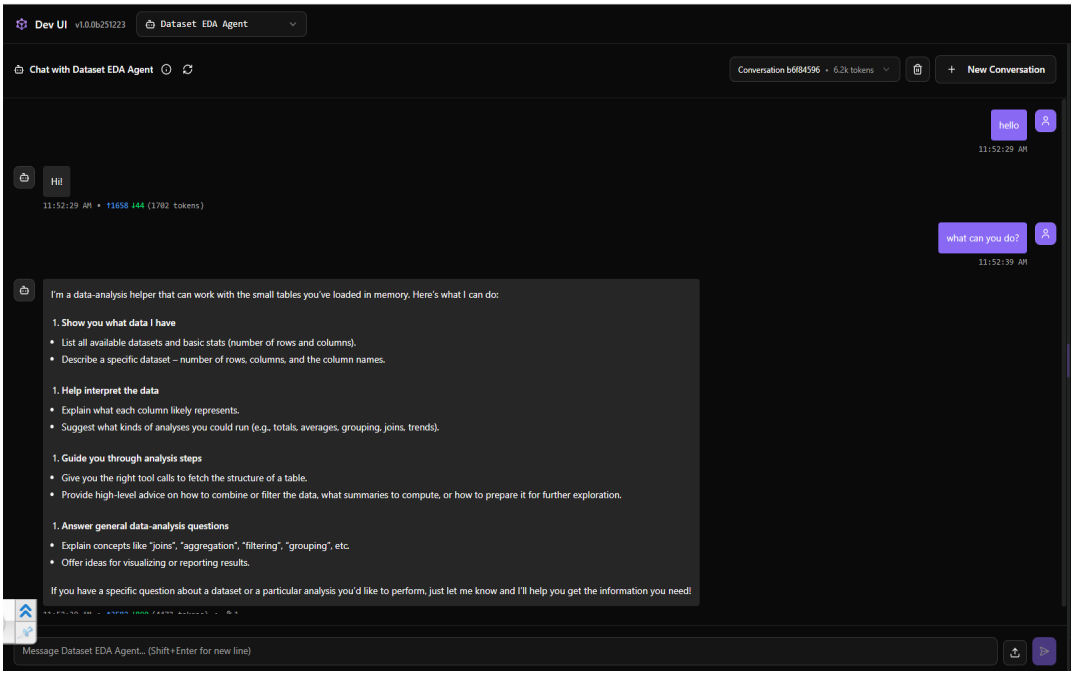
After building the image and running docker compose up -d, the container was successfully started. The deployment was validated by checking container status, logs, exposed ports, and environment variables.

Agent Functionality

The deployed agent exposes a DevUI interface that allows interactive communication with multiple agents. The system was adapted to our phishing-detection project, where email messages are analyzed for psychological manipulation patterns such as urgency, authority impersonation, and sensitive data requests.

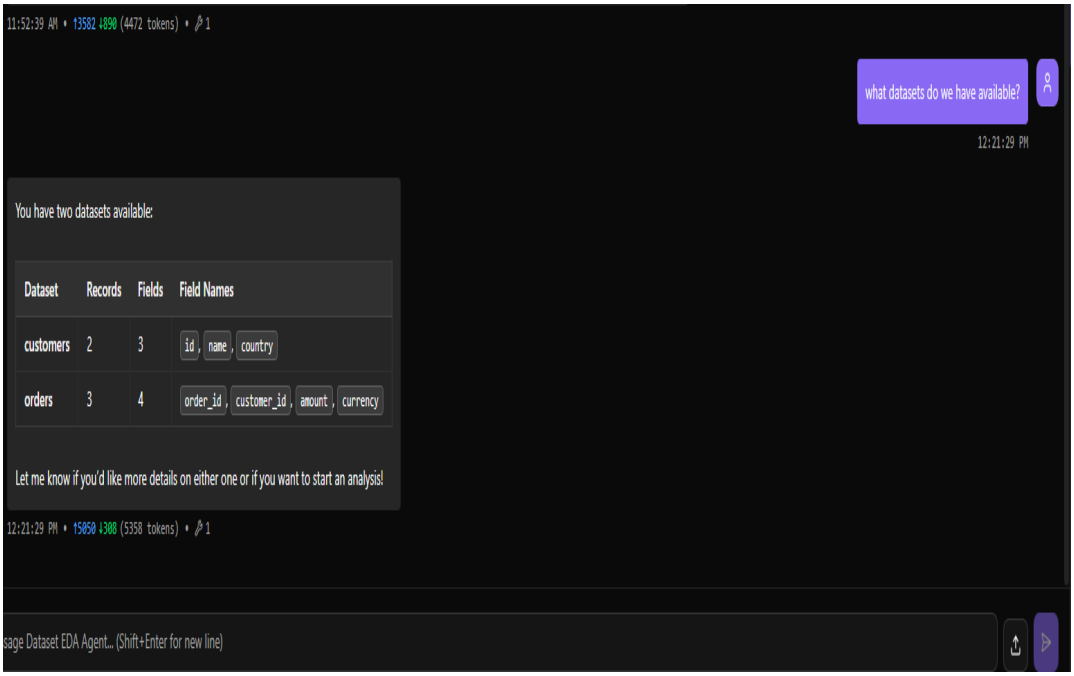
Appendix – Runtime Evidence





```
D:\CyberAI project\HIT-ai-cybersecurity-labs-main\labs\lab4 LLM Agent>docker images
REPOSITORY                TAG       IMAGE ID       CREATED          SIZE
cybersec-agent-devui      latest    1658bb58bdb1   28 minutes ago   1.24GB
redpandadata/console      latest    99043d88548f   40 hours ago     147MB
jaegertracing/all-in-one  latest    b0d7a1169c4c   6 weeks ago      85.2MB
jupyter/scipy-notebook    latest    ad65fcfebde3   2 years ago      4.14GB
confluentinc/cp-kafka     7.5.0     af34583c49f0   2 years ago      849MB
docker/getting-started    latest    3e4394f6b72f   3 years ago      47MB

D:\CyberAI project\HIT-ai-cybersecurity-labs-main\labs\lab4 LLM Agent>
```



```
D:\CyberAI project\HIT-ai-cybersecurity-labs-main\labs\lab4 LLM Agent>docker ps
CONTAINER ID   IMAGE              COMMAND             CREATED       STATUS       PORTS                              NAMES
cbec9da76c3e   cybersec-agent-devui   "uv run devui ./app …"   28 minutes ago   Up 28 minutes   0.0.0.0:8080->8080/tcp, :::8080->8080/tcp   cybersec-agent-devui


D:\CyberAI project\HIT-ai-cybersecurity-labs-main\labs\lab4 LLM Agent>
```

```
D:\CyberAI project\HIT-ai-cybersecurity-labs-main\labs\lab4 LLM Agent>docker exec -it cybersec-agent-devui env
PATH=/usr/local/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
HOSTNAME=cbec9da76c3e
TERM=xterm
API_KEY=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
ENABLE_SENSITIVE_DATA=true
API_BASE_URL=https://api.groq.com/openai/v1
MODEL=openai/gpt-oss-20b
ENABLE_OTEL=true
LANG=C.UTF-8
GPG_KEY=A035C8C19219BA821ECEA86B64E628F8D684696D
PYTHON_VERSION=3.11.14
PYTHON_SHA256=8d3ed8ec5c88c1c95f5e558612a725450d2452813ddad5e58fdb1a53b1209b78
UV_TOOL_BIN_DIR=/usr/local/bin
HOME=/root
```

```
D:\CyberAI project\HIT-ai-cybersecurity-labs-main\labs\lab4 LLM Agent>docker logs cybersec-agent-devui --tail 50
Using CPython 3.11.14 interpreter at: /usr/local/bin/python3
Creating virtual environment at: .venv
warning: Failed to hardlink files; falling back to full copy. This may lead to degraded performance.
         If the cache and target directories are on different filesystems, hardlinking may not be supported.
         If this is intentional, set `export UV_LINK_MODE=copy` or use `--link-mode=copy` to suppress this warning.
Installed 88 packages in 6.99s
[2026-01-15 09:51:33 - /app/.venv/lib/python3.11/site-packages/agent_framework_devui/__init__.py:131 - WARNING] ⚠️  WARNING: Exposing DevUI to network without authentication!
[2026-01-15 09:51:33 - /app/.venv/lib/python3.11/site-packages/agent_framework_devui/__init__.py:132 - WARNING] ⚠️  This is INSECURE - anyone on your network can access your agents
[2026-01-15 09:51:33 - /app/.venv/lib/python3.11/site-packages/agent_framework_devui/__init__.py:133 - WARNING] 🔒 For network exposure, add --auth flag: devui --host 0.0.0.0 --auth
INFO:     Started server process [28]
INFO:     Waiting for application startup.
INFO:     Application startup complete.
INFO:     Uvicorn running on http://0.0.0.0:8080 (Press CTRL+C to quit)
Agent Framework DevUI
==================================================
Entities directory: /app/app
Server URL: http://0.0.0.0:8080
UI enabled: Yes
Auto-reload: No
==================================================
Scanning for entities...
INFO:     127.0.0.1:54836 - "GET /health HTTP/1.1" 200 OK
INFO:     172.19.0.1:46312 - "GET / HTTP/1.1" 200 OK
INFO:     172.19.0.1:46312 - "GET /assets/index.js HTTP/1.1" 200 OK
INFO:     172.19.0.1:46316 - "GET /assets/index.css HTTP/1.1" 200 OK
INFO:     172.19.0.1:46312 - "GET /meta HTTP/1.1" 200 OK
INFO:     172.19.0.1:46312 - "GET /v1/entities HTTP/1.1" 200 OK
INFO:     172.19.0.1:46312 - "GET /v1/entities/dataset_eda/info?type=agent HTTP/1.1" 200 OK
INFO:     172.19.0.1:46316 - "GET /agentframework.svg HTTP/1.1" 200 OK
INFO:     172.19.0.1:46316 - "GET /v1/conversations?agent_id=dataset_eda HTTP/1.1" 200 OK
INFO:     172.19.0.1:46316 - "POST /v1/conversations HTTP/1.1" 200 OK
INFO:     172.19.0.1:46322 - "POST /v1/responses HTTP/1.1" 200 OK
INFO:     172.19.0.1:46322 - "POST /v1/responses HTTP/1.1" 200 OK
```