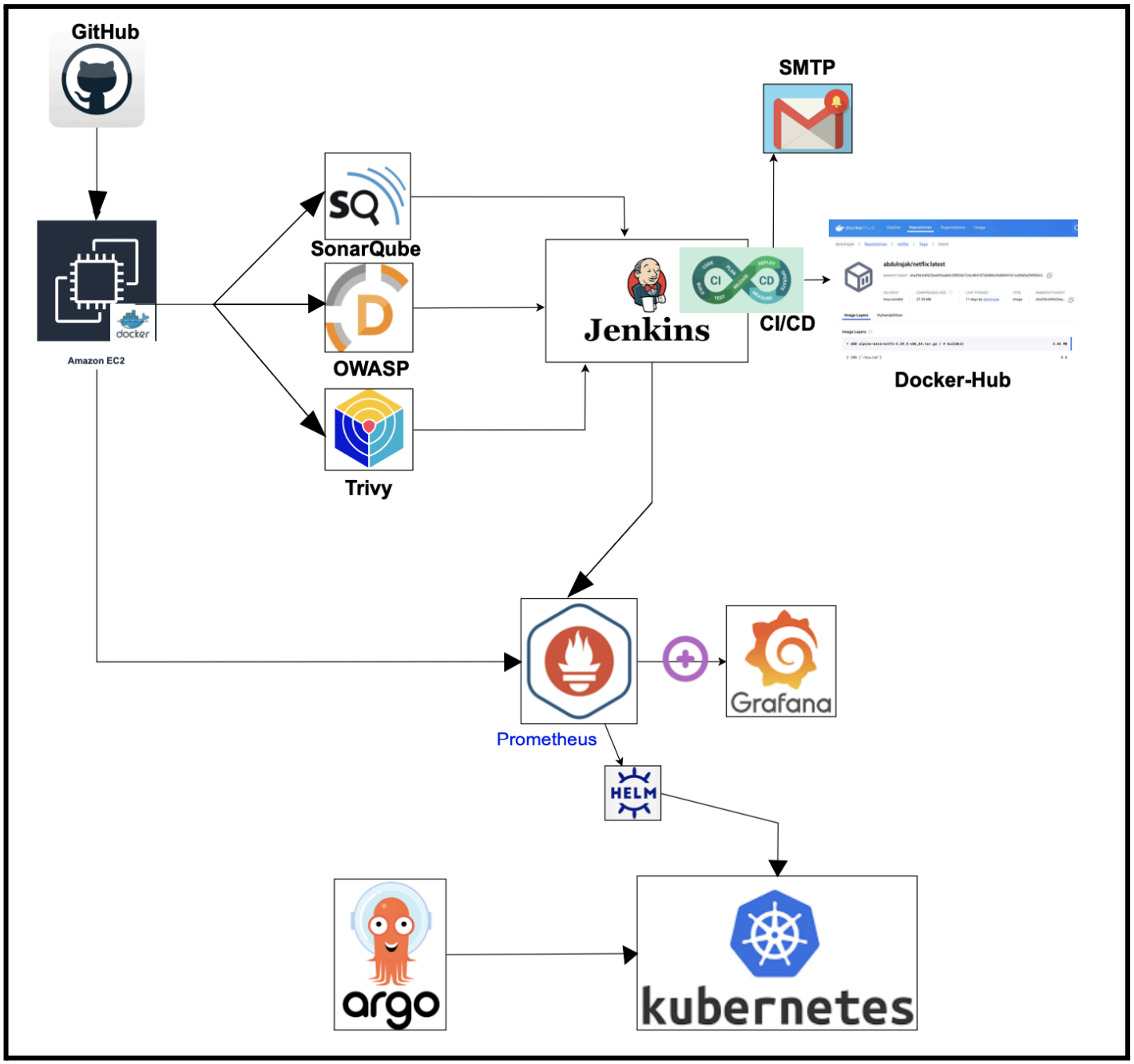
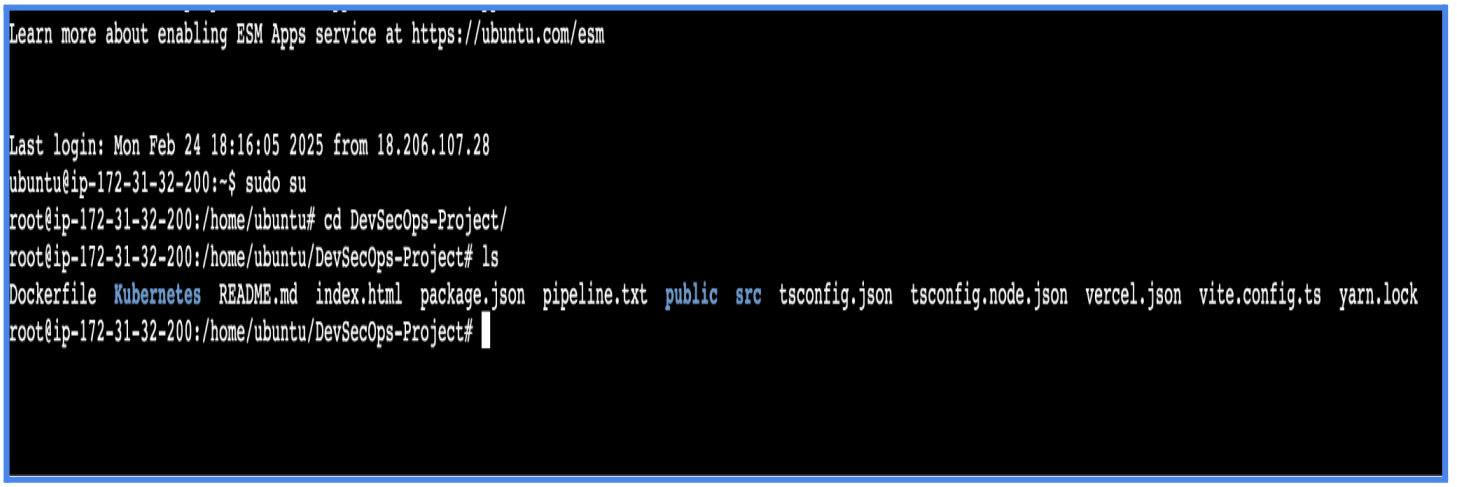
Deploying Netflix Clone on Cloud: A Complete DevSecOps Pipeline with Jenkins, GitHub, Docker, Amazon EC2, SonarQube, OWASP Dependency-Check, Trivy, ArgoCD, Helm, Kubernetes, Prometheus, Grafana, and Email Notifications!



Steps which I have followed for doing this task.

- **Initial Setup and Deployment**

  Created the t2.large instance to handle all the workload of the project and dependencies, and cloned the Git repository to EC2.



Create the API from TMDb.

~ TMDb (The Movie Database) is a popular online database for movies, TV shows, and celebrities, providing detailed information and metadata.

Data from TMDb is used to generate the API.

- **Create a Dockerfile, build the image using `docker build`, and test it locally using `docker run`.**

Phase CI/CD Setup

```
Dockerfile  Kubernetes  README.md  index.html  package.json  pipeline.txt
root@ip-172-31-32-200:/home/ubuntu/DevSecOps-Project# docker images
REPOSITORY            TAG               IMAGE ID       CREATED        SIZE
<none>                <none>            daa383d400ca   10 days ago    858MB
<none>                <none>            22bca05c40de   10 days ago    858MB
<none>                <none>            7f7bc33e038f   10 days ago    858MB
<none>                <none>            127d0261867b   10 days ago    858MB
<none>                <none>            e0f28b4958f9   11 days ago    858MB
abdulrajak/netflix    latest            12edfadc6b7f   11 days ago    56.5MB
netflix               latest            d9dd166a5970   13 days ago    56.5MB
<none>                <none>            a18b8b53fe50   13 days ago    844MB
nginx                 stable-alpine     bb941add9a4c   2 weeks ago    47.2MB
sonarqube             lts-community     522e1399903e   5 weeks ago    604MB
node                  16.17.0-alpine    5dcd1f6157bd   2 years ago    115MB
root@ip-172-31-32-200:/home/ubuntu/DevSecOps-Project#
```

Install Jenkins for Automation:

Installing Jenkins and configuring SonarQube, Trivy, and OWASP in Jenkins for CI/CD.

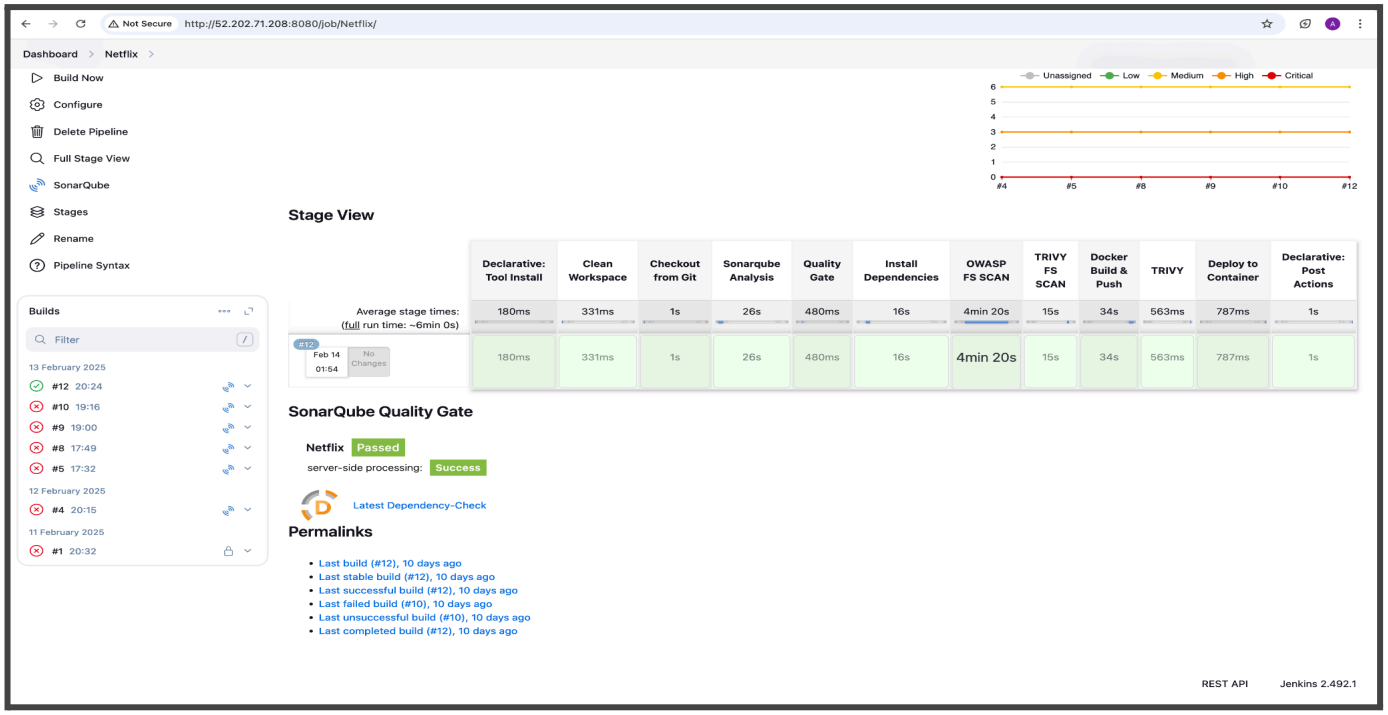
- Jenkins: An open-source automation server used for building, testing, and deploying applications in a CI/CD pipeline. It helps automate software development processes and integrates with various tools.
- SonarQube: A code quality and security analysis tool that scans code for vulnerabilities, bugs, and code smells. It ensures clean and maintainable code in the CI/CD pipeline.
- OWASP (Dependency-Check): A security tool that identifies known vulnerabilities in project dependencies. It helps mitigate security risks by ensuring third-party libraries are up to date and secure.

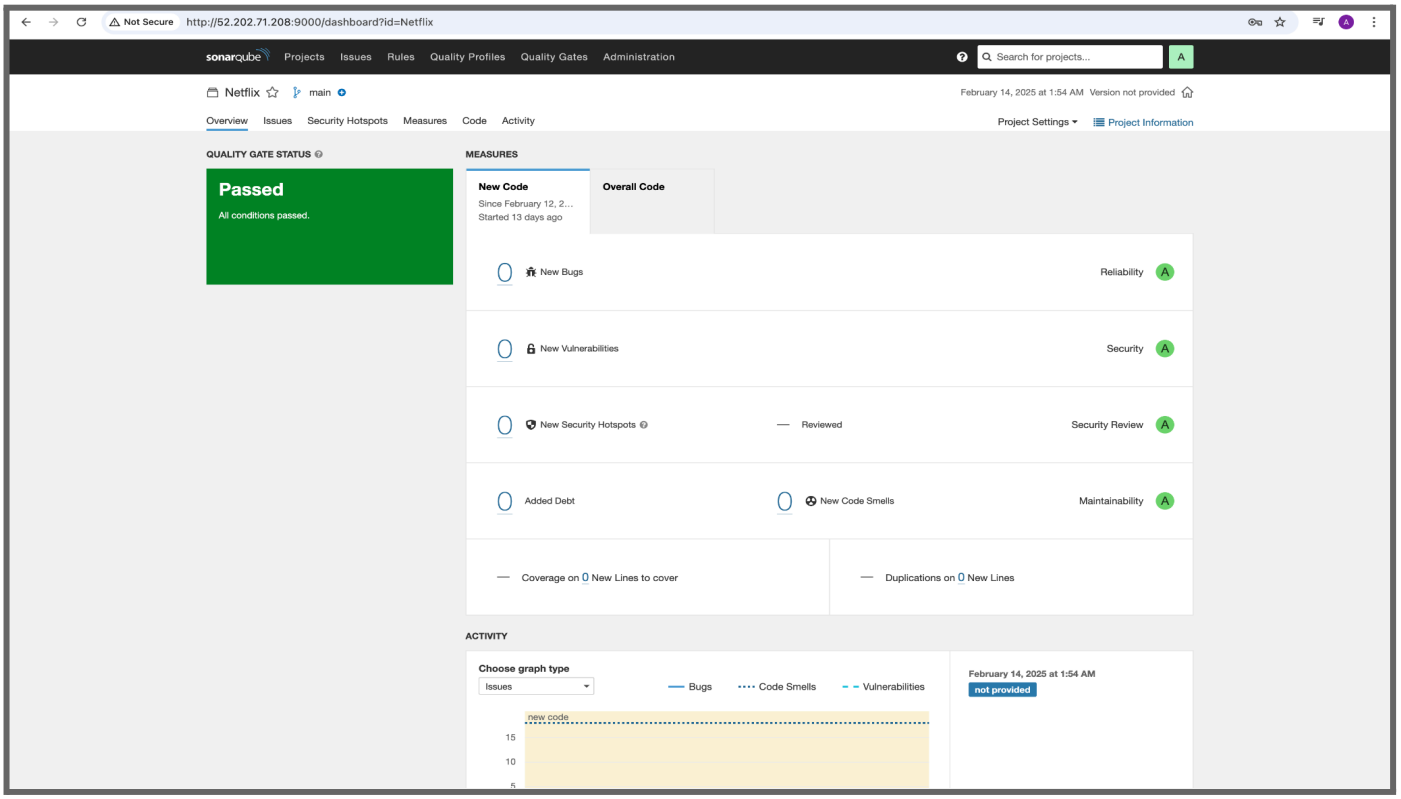
After successfully running the Jenkins pipeline, we can see the output like this:

Trivy is used in CI/CD for security and vulnerability scanning. Key reasons to use it:

- Container Security: Scans Docker images for vulnerabilities before deployment.
- Dependency Scanning: Detects security risks in open-source libraries and dependencies.
- Filesystem & Code Repository Scanning: Identifies misconfigurations and risks in infrastructure as code (IaC).

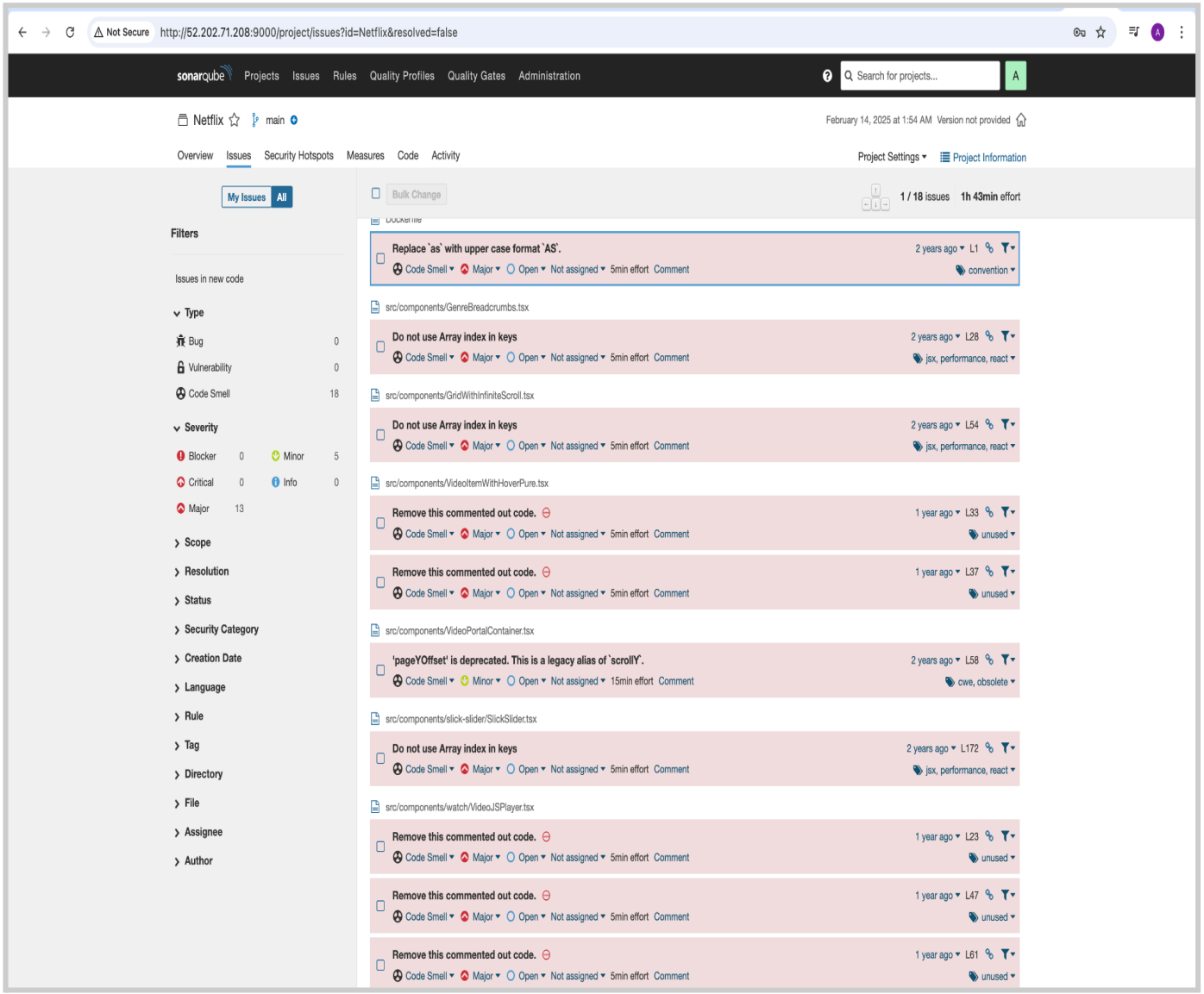
- Automation in CI/CD: Integrates with Jenkins, GitHub Actions, and other CI/CD tools for automated security checks.
- Compliance & Risk Management: Ensures applications meet security standards before production deployment.





SonarQube is used in CI/CD for code quality and security analysis. Key reasons to use it:

- Code Quality Analysis: Detects bugs, code smells, and maintainability issues in the codebase.
- Security Vulnerability Detection: Identifies security flaws like SQL injection and XSS in the code.
- Automated Code Review: Provides insights and recommendations to improve code quality.
- Seamless CI/CD Integration: Works with Jenkins, GitLab, and other CI/CD tools for continuous scanning.
- Compliance & Standards: Ensures adherence to coding standards and security best practices.

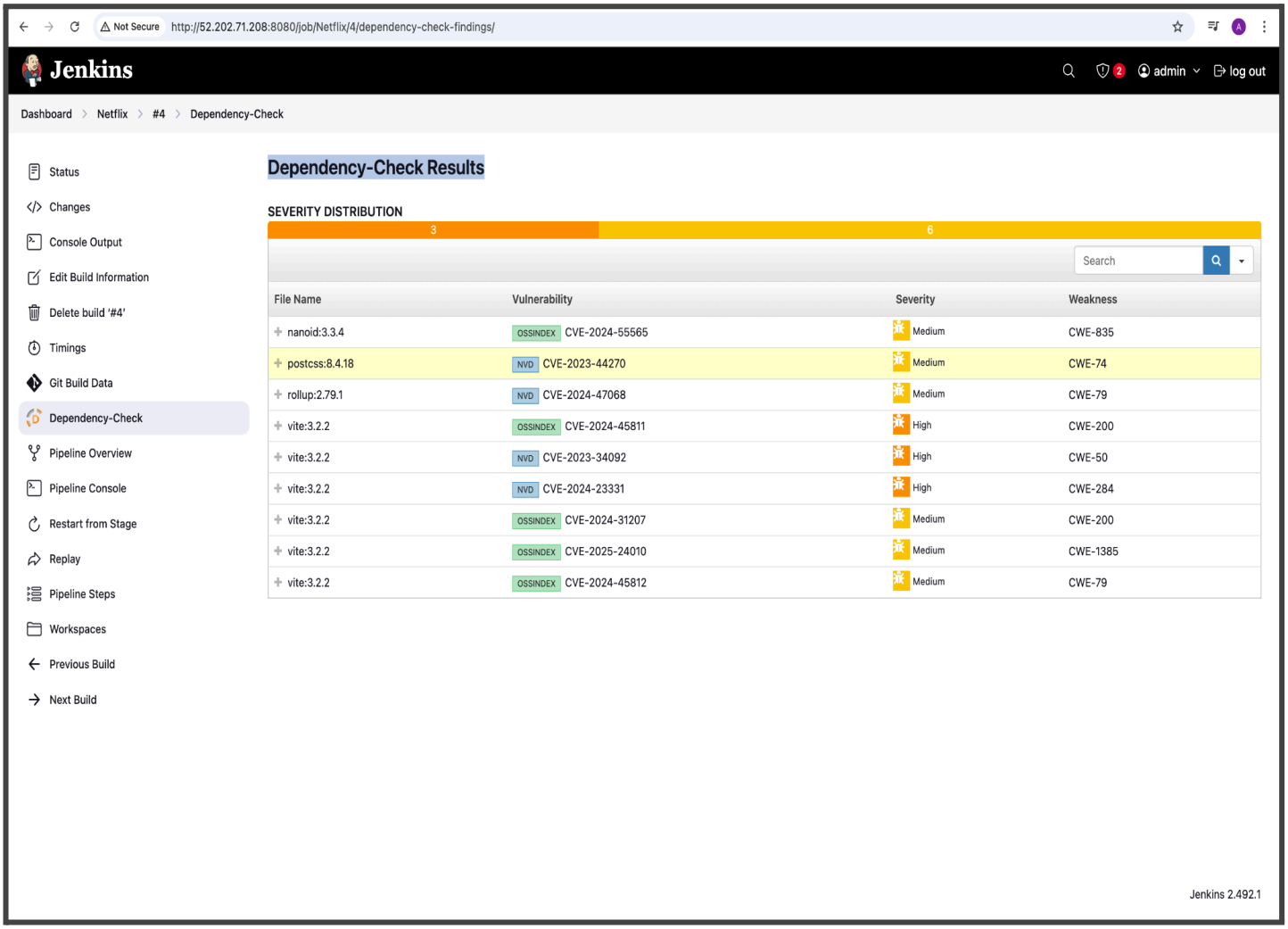


Trivy scans the entire image, including OS packages and application dependencies, to detect vulnerabilities. It categorizes findings by severity (Critical, High, Medium, Low) and provides a detailed report for security risk mitigation.

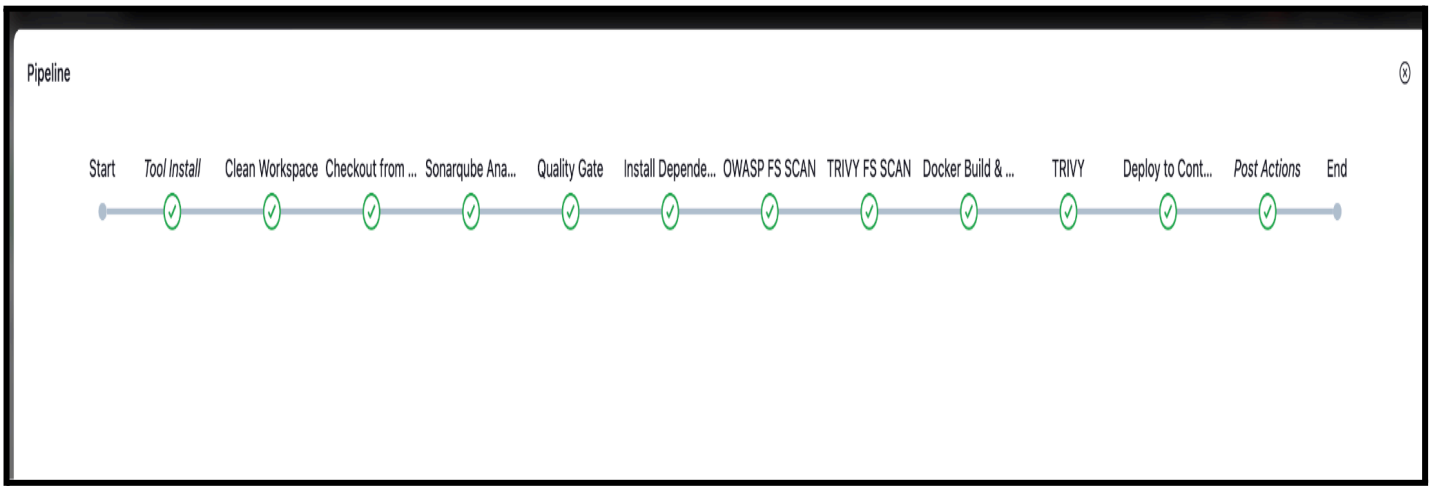
```
59.41 MiB / 59.41 MiB [-----------------------------------------------------------------------------------------------------------------------------------------------------------------------] 100.00% 25.80 MiB p/s 2.5s
2025-02-25T05:09:39Z    INFO    [vulndb] Artifact successfully downloaded       repo="mirror.gcr.io/aquasec/trivy-db:2"
2025-02-25T05:09:39Z    INFO    [vuln] Vulnerability scanning is enabled
2025-02-25T05:09:39Z    INFO    [secret] Secret scanning is enabled
2025-02-25T05:09:39Z    INFO    [secret] If your scanning is slow, please try '--scanners vuln' to disable secret scanning
2025-02-25T05:09:39Z    INFO    [secret] Please see also https://aquasecurity.github.io/trivy/v0.59/docs/scanner/secret#recommendation for faster secret detection
2025-02-25T05:09:41Z    INFO    Detected OS     family="alpine" version="3.20.5"
2025-02-25T05:09:41Z    INFO    [alpine] Detecting vulnerabilities...   os_version="3.20" repository="3.20" pkg_num=66
2025-02-25T05:09:41Z    INFO    Number of language-specific files       num=0
2025-02-25T05:09:41Z    WARN    Using severities from other vendors for some vulnerabilities. Read https://aquasecurity.github.io/trivy/v0.59/docs/scanner/vulnerability#severity-selection for details.

12edfadc6b7f (alpine 3.20.5)

Total: 12 (UNKNOWN: 4, LOW: 2, MEDIUM: 4, HIGH: 2, CRITICAL: 0)
```

Library	Vulnerability	Severity	Status	Installed Version	Fixed Version	Title
curl	CVE-2025-0725	MEDIUM	fixed	8.11.1-r0	8.12.0-r0	libcurl: Buffer Overflow in libcurl via zlib Integer Overflow https://avd.aquasec.com/nvd/cve-2025-0725
	CVE-2025-0167	LOW				When asked to use a `.netrc` file for credentials **and** to follow... https://avd.aquasec.com/nvd/cve-2025-0167
	CVE-2025-0665	UNKNOWN				libcurl would wrongly close the same eventfd file descriptor twice whe https://avd.aquasec.com/nvd/cve-2025-0665
libcrypto3	CVE-2024-12797	HIGH		3.3.2-r1	3.3.3-r0	openssl: RFC7250 handshakes with unauthenticated servers don't abort as expected https://avd.aquasec.com/nvd/cve-2024-12797
	CVE-2024-13176	MEDIUM			3.3.2-r2	openssl: Timing side-channel in ECDSA signature computation https://avd.aquasec.com/nvd/cve-2024-13176
libcurl	CVE-2025-0725			8.11.1-r0	8.12.0-r0	libcurl: Buffer Overflow in libcurl via zlib Integer Overflow https://avd.aquasec.com/nvd/cve-2025-0725
	CVE-2025-0167	LOW				When asked to use a `.netrc` file for credentials **and** to follow... https://avd.aquasec.com/nvd/cve-2025-0167
	CVE-2025-0665	UNKNOWN				libcurl would wrongly close the same eventfd file descriptor twice whe https://avd.aquasec.com/nvd/cve-2025-0665
libssl3	CVE-2024-12797	HIGH		3.3.2-r1	3.3.3-r0	openssl: RFC7250 handshakes with unauthenticated servers don't abort as expected https://avd.aquasec.com/nvd/cve-2024-12797
	CVE-2024-13176	MEDIUM			3.3.2-r2	openssl: Timing side-channel in ECDSA signature computation https://avd.aquasec.com/nvd/cve-2024-13176
musl	CVE-2025-26519	UNKNOWN		1.2.5-r0	1.2.5-r1	musl libc 0.9.13 through 1.2.5 before 1.2.6 has an out-of-bounds write https://avd.aquasec.com/nvd/cve-2025-26519
musl-utils						

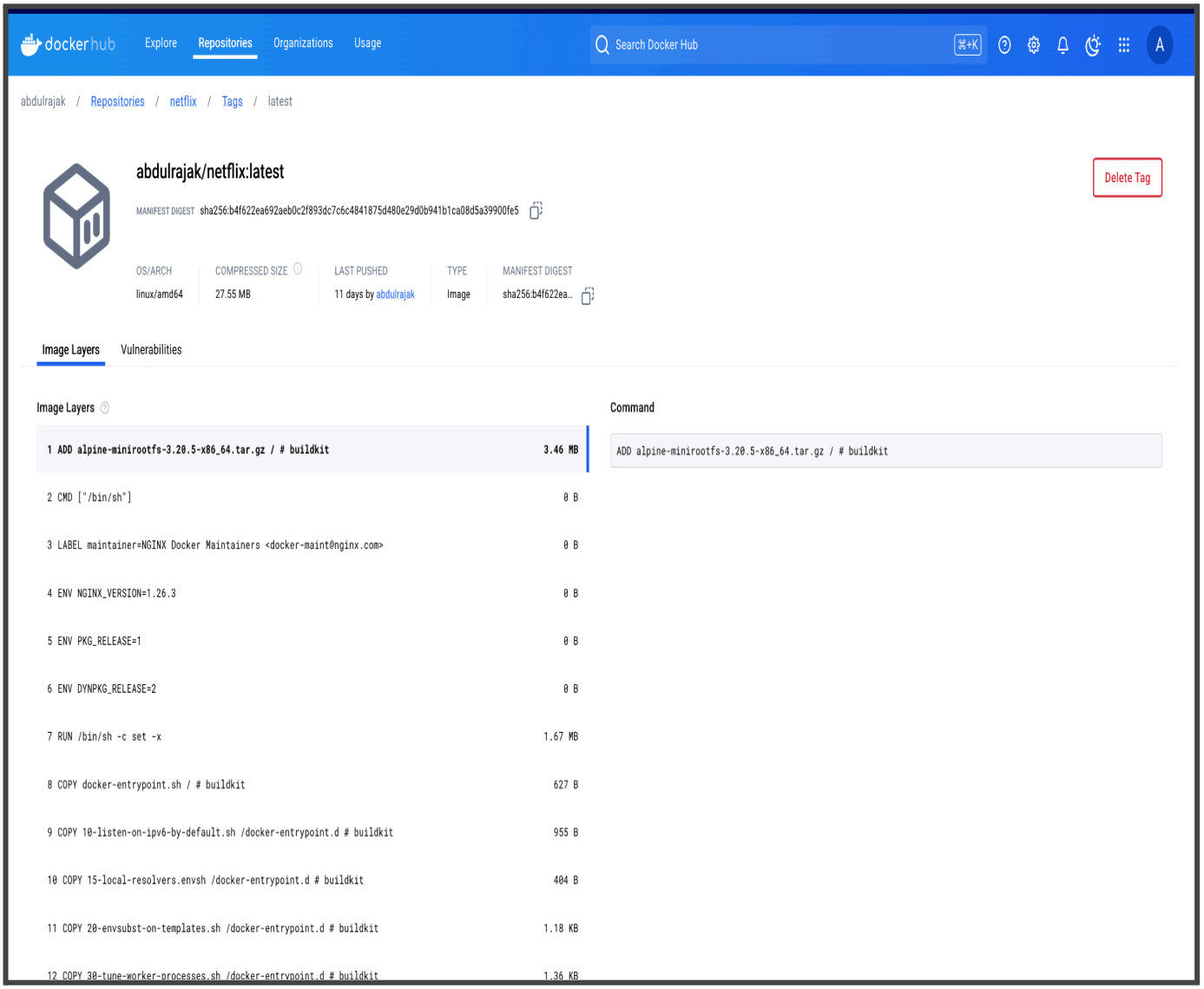
Dependency-Check Results



Pipeline overview



Docker images are pushed to Docker Hub in the specified repository using the `docker push` command after proper tagging. This ensures the image is stored remotely and can be pulled for deployment across different environments.



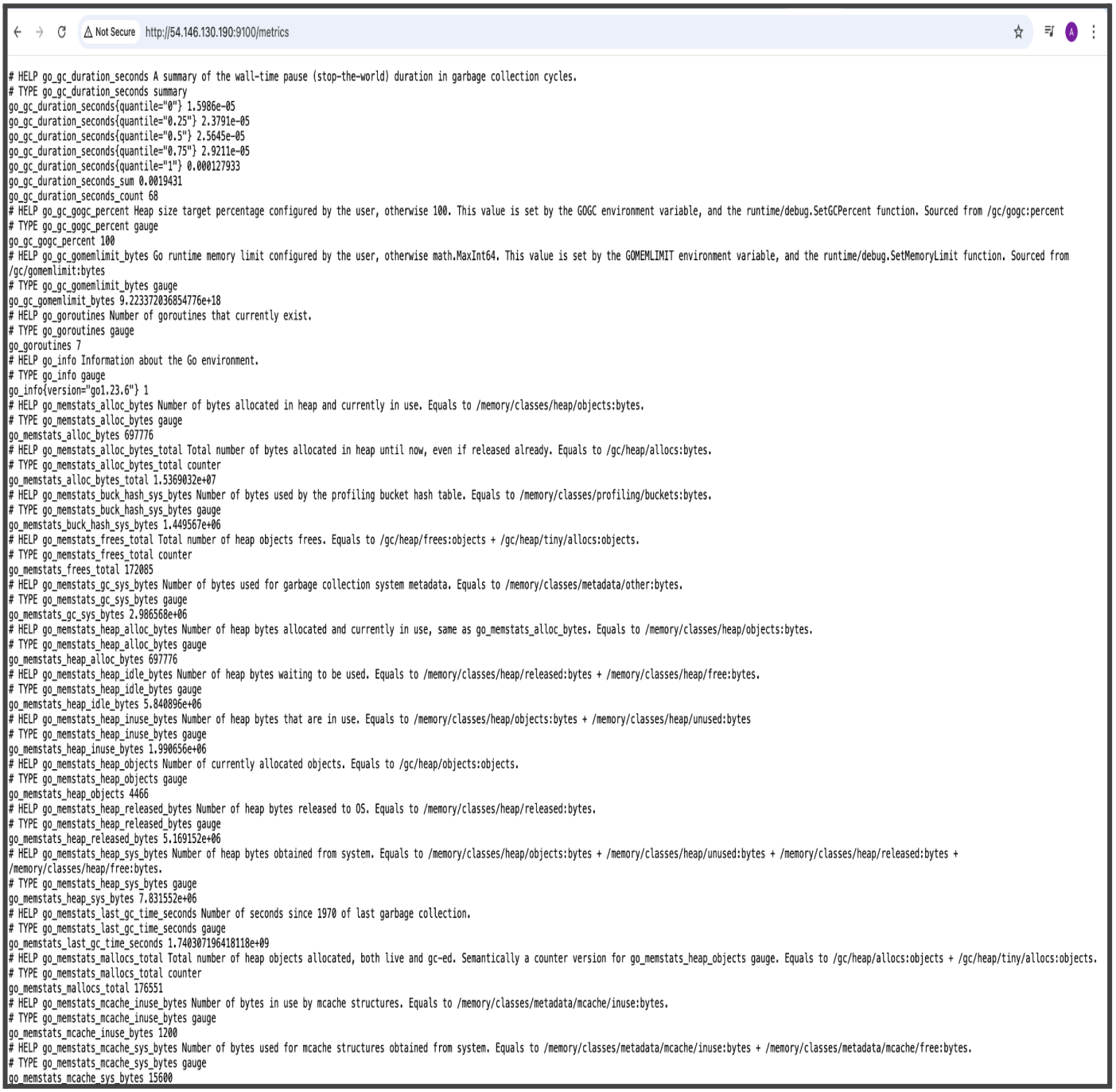
Phase Monitoring:

Node Exporter: Collects and exposes system-level metrics like CPU, memory, and disk usage. It runs as an agent on the server and depends on Prometheus to scrape and store these metrics. Without Node Exporter, Prometheus cannot collect server-level data.

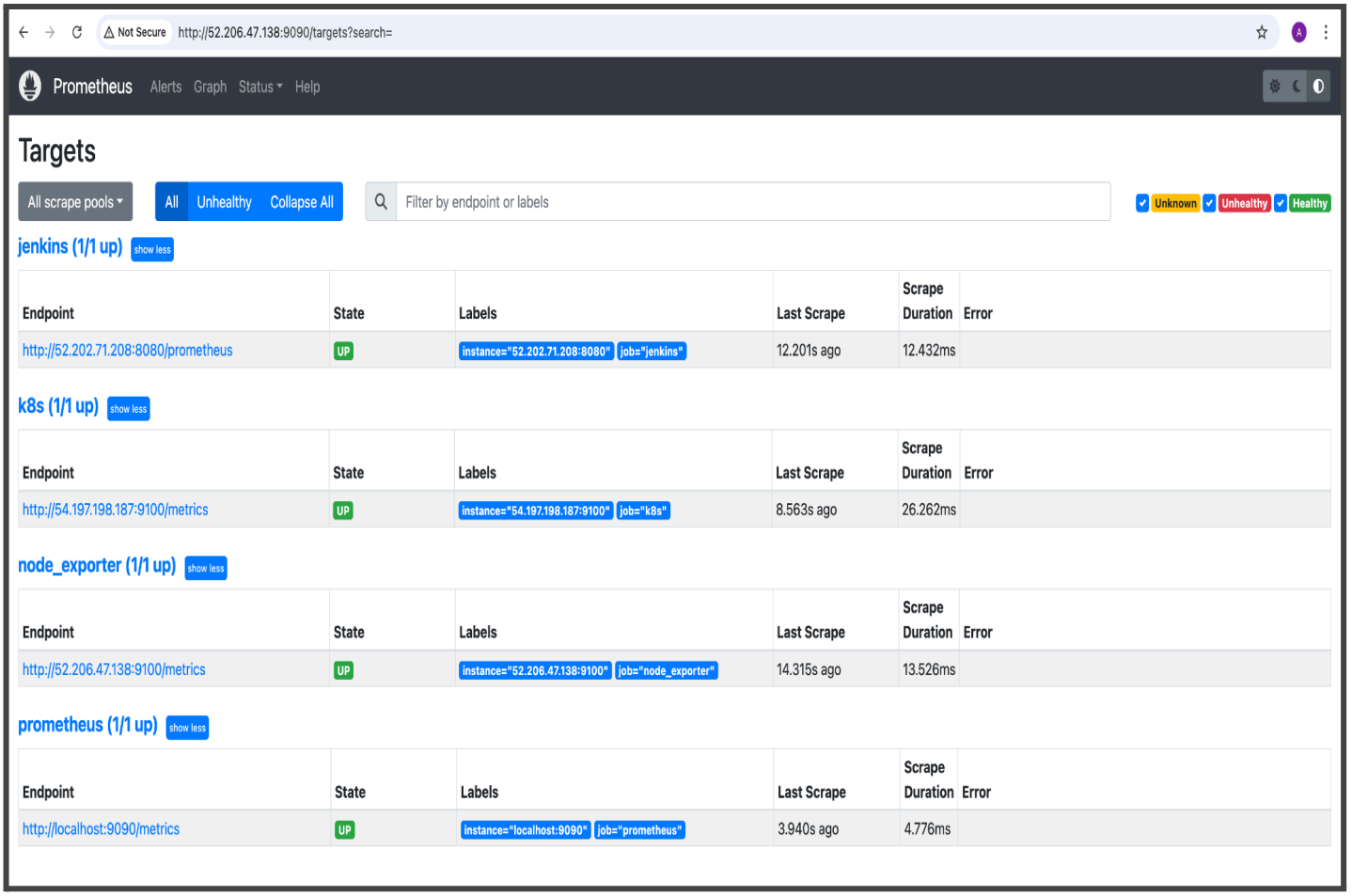
Metric Collection: Node Exporter gathers system-level metrics such as CPU, memory, disk, and network usage from the host machine.

Data Exposure: It makes these metrics available at `http://<server-ip>:9100/metrics` in a Prometheus-compatible format.

Integration with Prometheus: Prometheus scrapes these exposed metrics at regular intervals for monitoring and alerting.



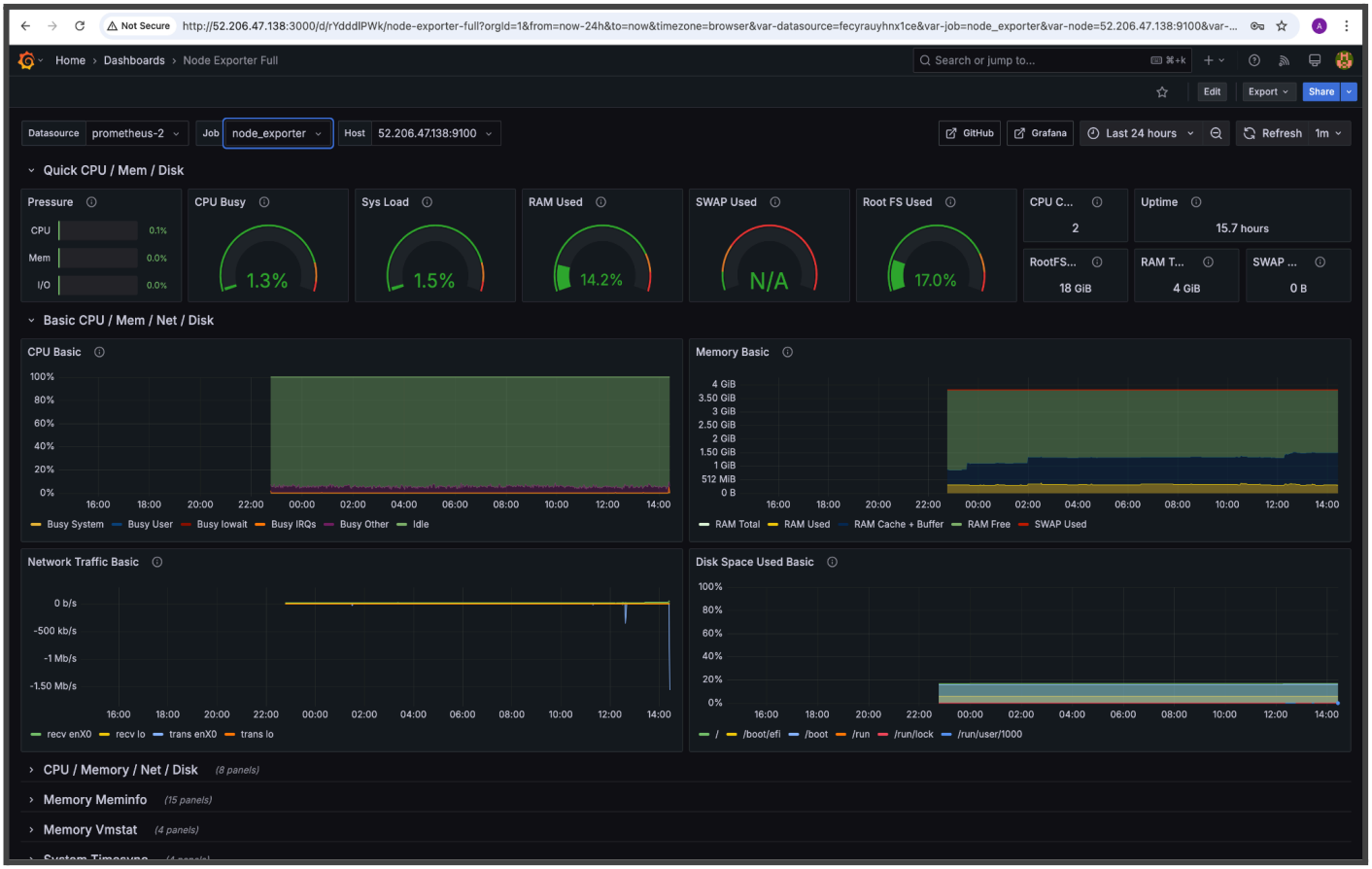
Prometheus: A monitoring system that scrapes metrics from Node Exporter and other sources, storing them as time-series data. It relies on exporters to gather data and depends on Grafana for visualization. Prometheus also provides querying and alerting capabilities.

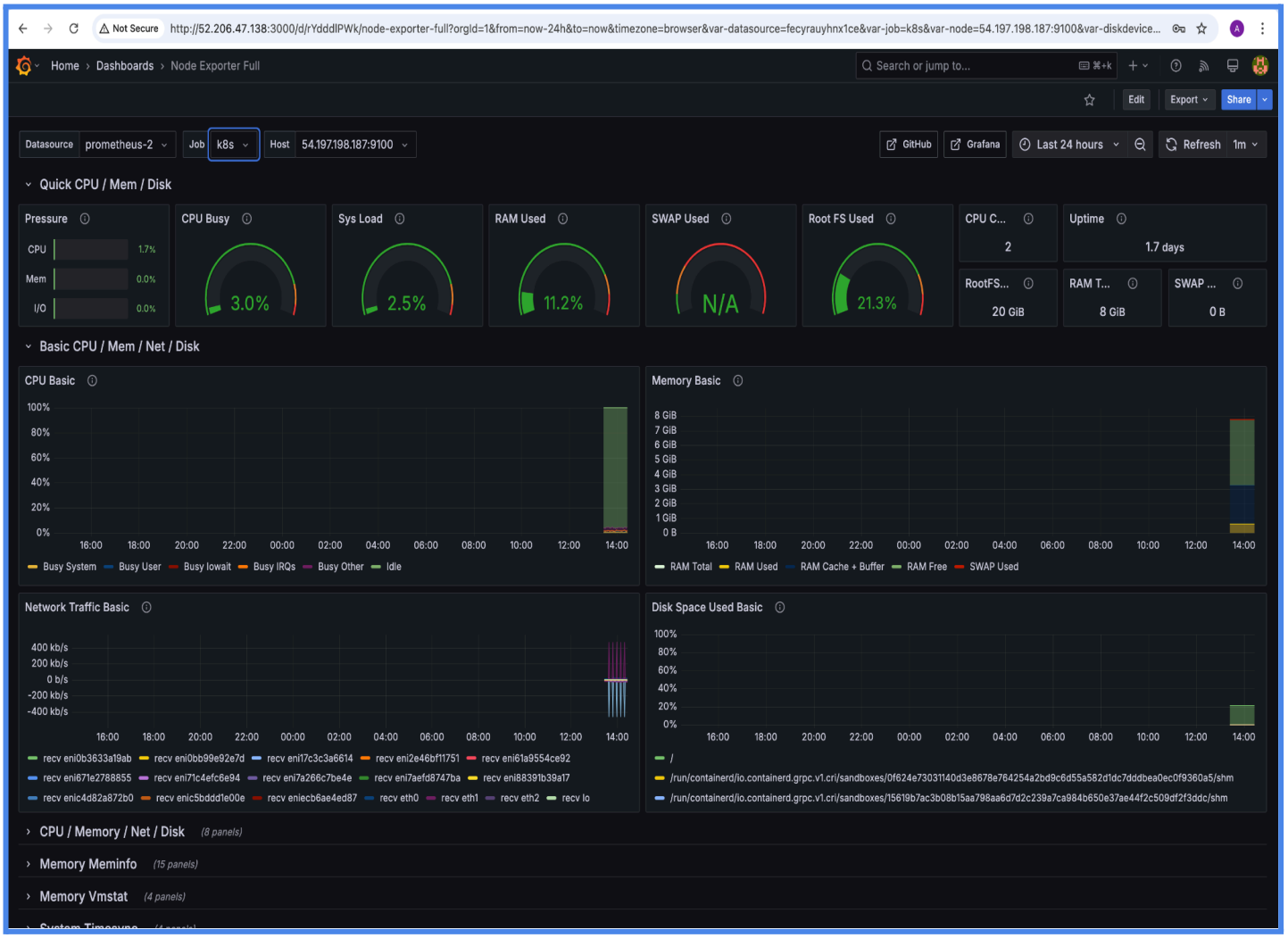


Extracted node metrics, including CPU, memory, and other system resources, using Node Exporter. The Prometheus container is running and scraping these metrics for monitoring. Additionally, services like Jenkins, Kubernetes, and other installed applications are also monitored through Prometheus.

Grafana is a visualization tool that provides interactive dashboards for monitoring metrics collected by Prometheus.

- It connects to Prometheus as a data source and queries stored metrics to generate real-time graphs and alerts.
- Grafana allows users to create custom dashboards with various panels, thresholds, and alerting rules.
- It supports multiple data sources, including Prometheus, Loki, Elasticsearch, and more.
- With role-based access control, teams can collaborate on monitoring and troubleshooting efficiently





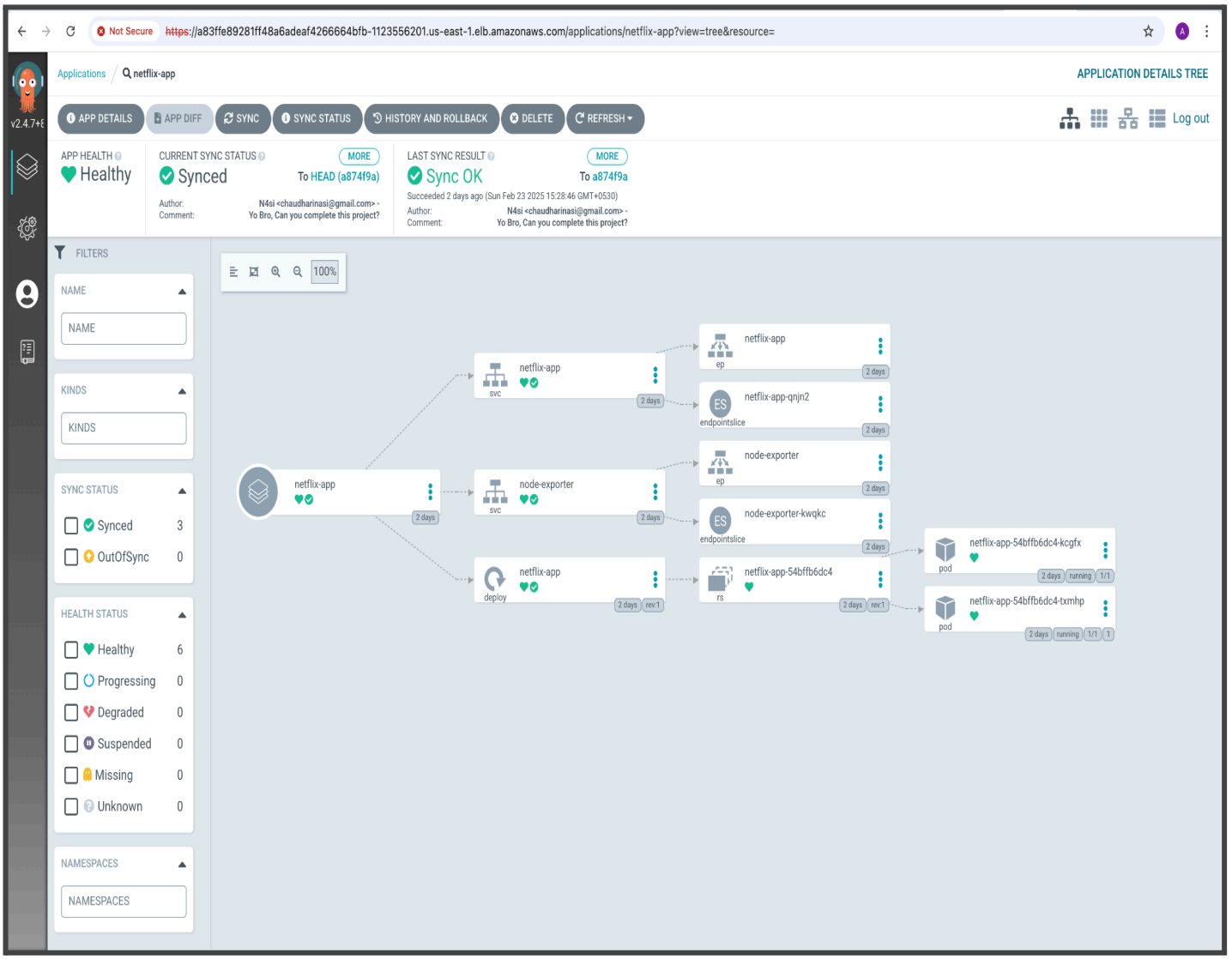
Docker hub :

abdulrajak/netflix:latest > Public Image

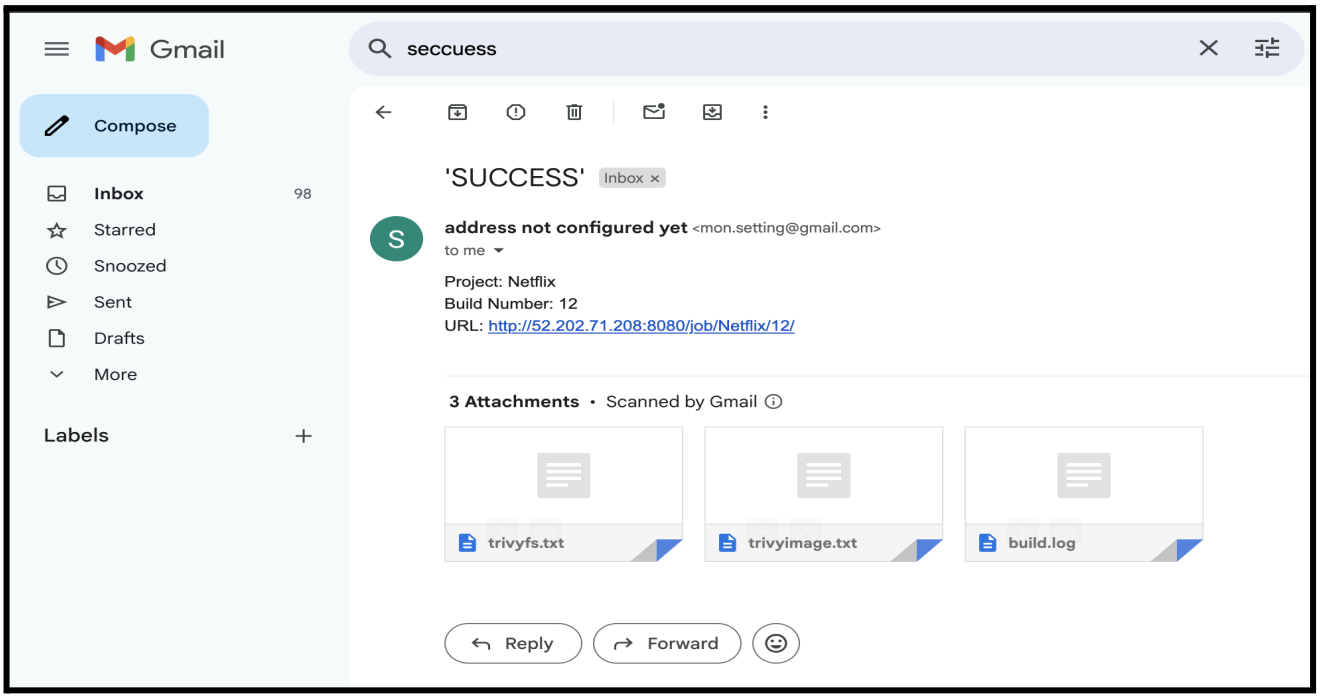
Argo CD is a declarative, GitOps-based continuous delivery tool for Kubernetes that automates application deployment and management. It ensures the cluster state remains in sync with the desired state defined in a Git repository.

Key Features:

- Automated Sync – Continuously syncs Kubernetes manifests from Git to maintain the desired state.
- Rollback & History – Supports rollbacks and maintains deployment history for quick recovery.
- Application Health Monitoring – Provides real-time visibility into application status and health.



After successfully completing the CI/CD pipeline at every stage, I integrated SMTP for email notifications. This setup ensures that Trivy scans images or containers and sends reports via email.




```
For OSS Maintainers: VEX Notice
--------------------------------
If you're an OSS maintainer and Trivy has detected vulnerabilities in your project that you believe are not actually exploitable, consider issuing a VEX
(Vulnerability Exploitability eXchange) statement.
VEX allows you to communicate the actual status of vulnerabilities in your project, improving security transparency and reducing false positives for your users.
Learn more and start using VEX: https://aquasecurity.github.io/trivy/v0.59/docs/supply-chain/vex/repo#publishing-vex-documents

To disable this notice, set the TRIVY_DISABLE_VEX_NOTICE environment variable.


package-lock.json (npm)
=======================
Total: 10 (UNKNOWN: 0, LOW: 0, MEDIUM: 7, HIGH: 3, CRITICAL: 0)

┌──────────┬────────────────┬──────────┬────────┬───────────────────┬──────────────────────────────┬──────────────────────────────────────────────────────────────┐
│ Library  │ Vulnerability  │ Severity │ Status │ Installed Version │        Fixed Version         │                            Title                             │
├──────────┼────────────────┼──────────┼────────┼───────────────────┼──────────────────────────────┼──────────────────────────────────────────────────────────────┤
│ esbuild  │ GHSA-67mh-4wv8-2f99 │ MEDIUM   │ fixed  │ 0.15.12           │ 0.25.0                       │ esbuild enables any website to send any requests to the      │
│          │                │          │        │                   │                              │ development server...                                        │
│          │                │          │        │                   │                              │ https://github.com/advisories/GHSA-67mh-4wv8-2f99            │
├──────────┼────────────────┼──────────┼────────┼───────────────────┼──────────────────────────────┼──────────────────────────────────────────────────────────────┤
│ nanoid   │ CVE-2024-55565 │          │        │ 3.3.4             │ 5.0.9, 3.3.8                 │ nanoid: nanoid mishandles non-integer values                 │
│          │                │          │        │                   │                              │ https://avd.aquasec.com/nvd/cve-2024-55565                   │
├──────────┼────────────────┼──────────┼────────┼───────────────────┼──────────────────────────────┼──────────────────────────────────────────────────────────────┤
│ postcss  │ CVE-2023-44270 │          │        │ 8.4.18            │ 8.4.31                       │ PostCSS: Improper input validation in PostCSS                │
│          │                │          │        │                   │                              │ https://avd.aquasec.com/nvd/cve-2023-44270                   │
├──────────┼────────────────┼──────────┼────────┼───────────────────┼──────────────────────────────┼──────────────────────────────────────────────────────────────┤
│ rollup   │ CVE-2024-47068 │ HIGH     │        │ 2.79.1            │ 3.29.5, 4.22.4, 2.79.2       │ rollup: DOM Clobbering Gadget found in rollup bundled        │
│          │                │          │        │                   │                              │ scripts that leads to...                                     │
│          │                │          │        │                   │                              │ https://avd.aquasec.com/nvd/cve-2024-47068                   │
├──────────┼────────────────┼──────────┼────────┼───────────────────┼──────────────────────────────┼──────────────────────────────────────────────────────────────┤
│ vite     │ CVE-2023-34092 │          │        │ 3.2.2             │ 2.9.16, 3.2.7, 4.0.5, 4.1.5, 4.2.3, 4.3.9 │ Vite Server Options (server.fs.deny) can be bypassed using   │
│          │                │          │        │                   │                              │ double forward-slash (//)                                    │
│          │                │          │        │                   │                              │ https://avd.aquasec.com/nvd/cve-2023-34092                   │
│          │                │          │        │                   │                              │
```

Finally, we can see the Netflix homepage deployed on Kubernetes (K8s) clusters.

Key Points:

- The deployment is managed via Argo CD for GitOps-based continuous delivery.
- Services are exposed using Kubernetes networking, ensuring accessibility.