Refer URL: <https://www.linkedin.com/pulse/what-trivy-rhythm-shahriar-vgyze>

**Trivy:**

* Trivy is an open-source security scanner designed to detect vulnerabilities in containers and other artifacts. It utilizes an internal database known as trivy-db, which houses detailed information about various vulnerabilities.
* It is developed and maintained by **[AquaSecurity](https://www.aquasec.com/?trk=article-ssr-frontend-pulse_little-text-block" \t "_blank)**
* Trivy not only scans for vulnerabilities but also provides suggestions for resolving the issues and links to detailed information about the vulnerabilities.
* Trivy can access extensive vulnerability information from various databases and utilizes this data to identify security issues. Among the databases it draws from are the National Vulnerability Database (NVD), Red Hat Security Data, and Alpine SecDB.
* During a scan, Trivy compares the software packages and libraries in a directory or container image with its vulnerability database. If a match is found, indicating a vulnerability, Trivy reports the issue along with details such as severity level, affected versions, and recommended fixes.
* Trivy updates its database every six hours. When you initiate a scan, Trivy automatically updates the database, eliminating the need for you to manually track updates.

**Install Trivy:**

Let’s see how to install Trivy on Ubuntu, follow the below steps to install Trivy.

For other platform, please visit the [**official installation page.**](https://aquasecurity.github.io/trivy/v0.18.3/installation/?trk=article-ssr-frontend-pulse_little-text-block)

* **Step 1:** First, install the required dependencies for Trivy using the command given below:

- sudo apt-get install wget apt-transport-https gnupg lsb-release

* **Step 2**: Download the public key and Trivy repository using the commands given below:

- wget -qO - https://aquasecurity.github.io/trivy-repo/deb/public.key | gpg --dearmor | sudo tee /usr/share/keyrings/trivy.gpg > /dev/null

- echo "deb [signed-by=/usr/share/keyrings/trivy.gpg] https://aquasecurity.github.io/trivy-repo/deb $(lsb\_release -sc) main" | sudo tee -a /etc/apt/sources.list.d/trivy.list

* **Step 3**: Update the repository using the update command.

sudo apt update -y

Step 4: Install Trivy using the command:

sudo apt install trivy

To verify the installation and understand all the available option, run the following trivy help command.

trivy -h

You should get an output a shown below.

trivy -h

Scanner for vulnerabilities in container images, file systems, and Git repositories, as well as for configuration issues and hard-coded secrets

Usage:

trivy [global flags] command [flags] target

trivy [command]

Examples:

# Scan a container image

$ trivy image python:3.4-alpine

# Scan a container image from a tar archive

$ trivy image --input ruby-3.1.tar

# Scan local filesystem

$ trivy fs .

# Run in server mode

$ trivy server

Scanning Commands

aws [EXPERIMENTAL] Scan AWS account

config Scan config files for misconfigurations

filesystem Scan local filesystem

image Scan a container image

kubernetes [EXPERIMENTAL] Scan kubernetes cluster

repository Scan a remote repository

rootfs Scan rootfs

sbom Scan SBOM for vulnerabilities

vm [EXPERIMENTAL] Scan a virtual machine image

Management Commands

module Manage modules

plugin Manage plugins

Utility Commands

completion Generate the autocompletion script for the specified shell

convert Convert Trivy JSON report into a different format

help Help about any command

server Server mode

version Print the version

Flags:

--cache-dir string cache directory (default "/Users/bibinwilson/Library/Caches/trivy")

-c, --config string config path (default "trivy.yaml")

-d, --debug debug mode

-f, --format string version format (json)

--generate-default-config write the default config to trivy-default.yaml

-h, --help help for trivy

--insecure allow insecure server connections

-q, --quiet suppress progress bar and log output

--timeout duration timeout (default 5m0s)

-v, --version show version

Use "trivy [command] --help" for more information about a command.

**Using Trivy To Scan for Vulnerability**

Whenever you run the Trivy command to scan for vulnerabilities, it will first download the relevant database and then compare your software against the vulnerabilities listed in it.

Trivy shows the risk of vulnerability as critical, high, medium, and low.

1. Critical – This is the most severe vulnerability which needs to be fixed as soon as possible because it can allow administrative control over the system.
2. High – It could cause data leakage.
3. Medium – It could make the system unavailable for users.
4. Low – This can be solved during regular maintenance.

We can use Trivy to scan the following targets:

1. Container images
2. Filesystem
3. Remote Git repositories

There are also experimental features to scan [**Kubernetes**](https://devopscube.com/kubernetes-tutorials-beginners/?trk=article-ssr-frontend-pulse_little-text-block) & AWS configurations.

Trivy uses different commands to scan targets that are mentioned above.

Let’s look at an example for each.

**Scan Container Images**

You can scan container images for vulnerabilities using Trivy.

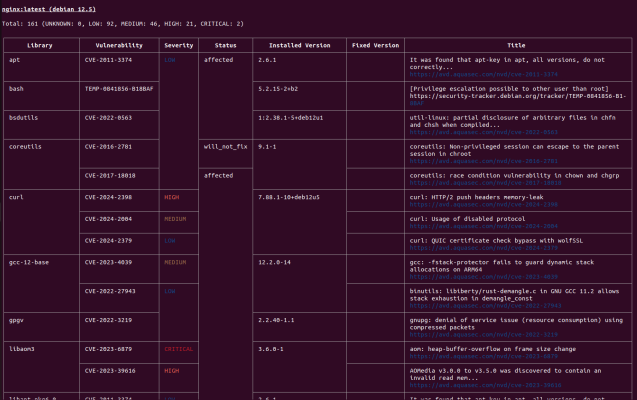
The command used to scan container images is given below:

trivy image <image name>

For example, if the name of the image is nginx:latest then the command will be:

trivy image nginx:latest

It will scan the image and shows the vulnerability of the image as shown below.



If you have the container image in tar format, you can use the following command to scan it.

trivy image --input nginx:latest.tar

**Scan Filesystem**

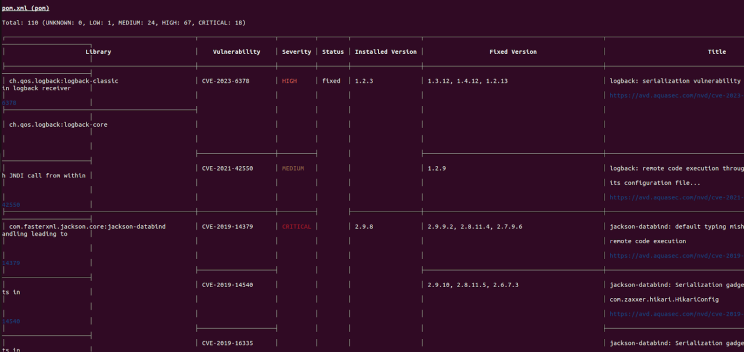
The command used to scan the filesystem is given below:

trivy fs <path of the directory>

For example, if the path of the directory is Documents/java-application/ then the command will be:

trivy fs Documents/java-application

It will scan the directory and shows the vulnerability in the directory as shown below.



**Scan Git Repository**

The command used to scan the git repository is given below:

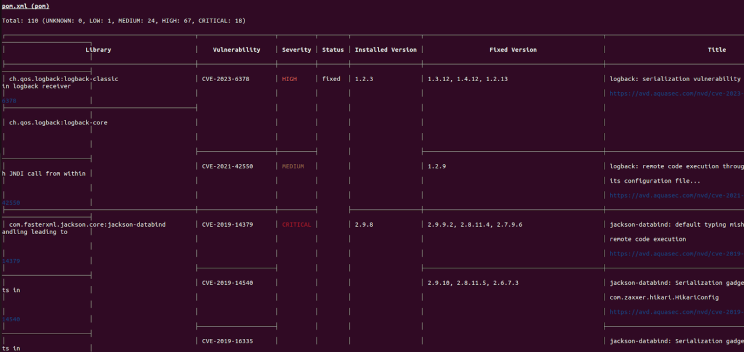
trivy repo <repo URL>

If you are using a private repository, you need to provide your git token for authentication as given below.

export GITHUB\_TOKEN=<git token>

trivy repo <repo URL>

It will scan the repo and shows the vulnerability in the repo as shown below.



**Conclusion**

Vulnerability scanning is a crucial aspect of CI/CD. During the CI stages, it's essential to scan application code, infrastructure code, and configuration files for vulnerabilities. This practice is key to maintaining strong DevSecOps standards.