A black and white logo

Description automatically generated with low confidence

|  |  |
| --- | --- |
| Document name | DevSecOps Tool: Trivy User Guide |
| Version no. | 1.0 |
| Release date | 12th oct 2023 |
| Document ID | *1* |
| Classification | Internal |

|  |
| --- |
| DevSecOps Tool: Trivy User Guide |

# Document History

| Ver. No | Release Date | Created By / Modified By and Date | Reviewed By and Date | Approved By and Date | Remarks and Changes Made |
| --- | --- | --- | --- | --- | --- |
| 1.0 | 12tth Oct 2023 | Ruturaj Kharde / 12th Oct 2023 | Prasad Gattetwar and Rajanigandha Gaikwad /5th Dec 2023 |  |  |

# Table of Contents

[Document History 2](#_Toc152676996)

[Table of Contents 3](#_Toc152676997)

[1. scaN and Code Coverage using cli 4](#_Toc152676998)

[1.1 SUPPORTED OPERATION SYSTEMS 4](#_Toc152676999)

[1.2 SUPPORTED TARGETS 4](#_Toc152677000)

[1.3 WHAT IT SCANS 4](#_Toc152677001)

[2. TRIVY WITH WINDOWS OS 5](#_Toc152677002)

[2.1 INSTALLATION 5](#_Toc152677003)

[2.2 SCANNING PROJECT LOCALLY 5](#_Toc152677004)

[2.3 SCANNING REPOSITORY 6](#_Toc152677005)

[2.4 SCANNING PROJECT FROM PIPELINE ON SELF HOSTED AGENT 6](#_Toc152677006)

[2.5 LIMITATIONS 6](#_Toc152677007)

[3. References 7](#_Toc152677008)

# scaN and Code Coverage using cli

## **SUPPORTED OPERATION SYSTEMS**

Trivy tool is open source and available on website <https://github.com/aquasecurity/trivy> .It is cross platform tool can easily work for OS as

* Linux
* Ubuntu
* windows
* mac
* Docs

## **SUPPORTED TARGETS**

Trivy (pronunciation) is a comprehensive and versatile security scanner. Trivy has scanners that look for security issues, and targets where it can find those issues**.**

* Container Image
* Filesystem
* Git Repository (remote)
* Virtual Machine Image
* Kubernetes
* AWS

## **WHAT IT SCANS**

Scanners (what Trivy can find there):

* OS packages and software dependencies in use (SBOM)
* Known vulnerabilities (CVEs)
* IaC issues and misconfigurations
* Sensitive information and secrets
* Software licenses

Trivy supports most popular programming languages, operating systems, and platforms. For a complete list, see the Scanning Coverage page.

We will be discussing how to scan the **file system** scanning on **windows** using Trivy

# TRIVY WITH WINDOWS OS

## **INSTALLATION**

**Step 1**. Open PowerShell in admin mode

**Step 2**. Download the tool from website using command *git clone --depth 1 --branch v0.46.0* [*https://github.com/aquasecurity/trivy*](https://github.com/aquasecurity/trivy)

**Step 3**. A folder will be created navigate PS in folder trivy using command *cd trivy*

**Step 4**. Check whether go language is installed or not by typing *go on PS*

**Step 5**. If go language is not installed open official website [*https://go.dev/dl/*](https://go.dev/dl/)and download .msi file and install it.

**Step 6**. According to installation folder, navigate to the bin folder of go language and set its path to path variable in environment variable section.

**Step 7**. Execute the trivy installation command *go install ./cmd/trivy*

## **SCANNING PROJECT LOCALLY**

**Step 1**. Navigate to the root of the Filesystem/project.

**Step 2**. Open CLI

**Step 3**. Now to do the analysis, there are different commands which will output the same results in different format.

*Trivy Filesystem .* – will scan the project vulnebraties and display the result on CLI in from of table

*trivy fs --format json -o JSON\_REPORT.json . -* will scan the project vulnebraties and display the result in json file at root of the project in from of json

*trivy fs --format table -o TABLE\_REPORT.txt . -* will scan the project vulnebraties and display the result in txt file at root of the project in from of table

*trivy fs --format sarif -o SARIF\_REPORT.sarif . - w*ill scan the project vulnebraties and display the result in sarif file at root of the project in from of sarif

## **SCANNING REPOSITORY**

**Step 1**. Open CLI in admin mode

**Step 2**. To scan vulnebraties of a complete repo use command *trivy repo <repo url>*

**Step 3**. To scan a specific branch vulnebraties from repo *trivy repo --branch <branch-name> <repo-url>*

## **SCANNING PROJECT FROM PIPELINE ON SELF HOSTED AGENT**

**Step 1.** Add the file called trivy.exe in Agent.ToolsDirectory (which is tool folder in agent’s work directory)

**Step 2.** Add the task of CLI in pipeline just before the build task.

**Step 3.** Add the below command set in the task

cd $(Agent.ToolsDirectory)

# TABLE format

./trivy fs $(System.DefaultWorkingDirectory)

**step 4.** Run the pipeline and results will be displayed in task log

## **LIMITATIONS**

1. If project size is increasing, scanning of the project takes too long time.
2. If we want to exclude any of the file from scan, no mechanism is available

# References

https://aquasecurity.github.io/trivy/v0.47/ecosystem/prod/